Chapter 12

The State Role in Privacy Protection

Naming the new nation the "United States of America" reflected the founders' commitment to the Federal Principle, the division of power between the States and the national government. From the beginning, each State was, and still is, a sovereign authority, with power to perform within its borders almost all of the activities, legislative, executive, and judicial, that the Federal government performs, except to represent itself in foreign affairs, burden interstate commerce, and provide for the national defense. It can, and does, tax its citizens, provide services, regulate commerce, license professions, and exercise police powers. Indeed, the national government was intended to be the government of limited, delegated powers, with the States exercising domestically, any of the powers one might expect a government to use. That was the theory, though in practice the pendulum has gradually swung so that the Federal government is now the forum where the great domestic policy issues, social as well as economic, are resolved. The States' role is still important, and shows signs of growing, but currently is the more limited one. The State still functions as a basic provider of government services, but in many cases is simply carrying out programs that originate at the national level and are funded, at least in part, by the Federal government. Even in the sectors it controls, for example, police protection, Federal statutory programs carried out by agencies like the Law Enforcement Assistance Administration (LEAA) are beginning to make inroads on its authority. The States are still the governmental vehicle for determining land use and allocation of most of the natural resources within their borders; though, once again, the Federal government has begun to take a prominent role in order to assure environmental quality and effect national resource policies. Population growth, urbanization, mobility, and economic integration have turned many of the social and economic problems that could once be managed at the local level into problems that require national attention. Thus, the Federal government, of necessity, now dominates many areas that were traditionally State preserves.

The role of State governments in protecting personal privacy is, however, still enormously important. The records a State government keeps about the individuals under its jurisdiction are often as extensive as those kept on the same individuals by the Federal government, and in some respects even more so. As a prelude to the following chapters which consider various aspects of the relationship between the individual and agencies of the Federal government, this chapter briefly summarizes how the Federal-

State relationship enters into the Commission's recommended program for protecting personal privacy. Four aspects of that relationship are important to the national policy the Commission proposes:

- How the Federal government constrains State activities;
- How States have tried to protect personal privacy;
- How State record-keeping practices affect personal privacy; and
- How the Commission's recommendations fit into the existing system for implementing national policy at the State level.

Federal Constraints on State Activities

The Federal government may restrict State action or take action itself affecting apparently intrastate activity on the basis of four Constitutional provisions: the commerce clause, the spending clause, the Fourteenth Amendment, and the welfare clause. The commerce clause enables the Federal government to regulate interstate commerce by precluding certain State regulation. In legislating under the commerce clause, however, the Congress sometimes explicitly leaves existing State regulation intact, or provides that States may also regulate, so long as State regulation does not conflict with existing Federal law. For example, Federal and State Fair Credit Reporting Acts and the existing banking system provide for dual regulatory structures in those areas. In fact, only in limited areas such as trademark and copyright law has the Federal government prohibited the States from acting. Congress has also used the commerce clause, alone or in conjunction with the Fourteenth Amendment, as its authority for enacting some laws that are basically social legislation, for example, the Equal Credit Opportunity Act, the Civil Rights Act of 1964, and the Equal Employment Opportunity Act.

The Fourteenth Amendment, mainly through its equal protection clause, enables the Congress to limit State regulation in areas of social policy, but it is the combination of the welfare and spending clauses that gives the Congress most of its power to affect social issues and limit State action that affects them. Federal programs predicated on the spending power can either restrict or require State action, or both. The Medicaid program, for example, requires the States to maintain certain records about individuals and restricts the disclosure of that information. The constraints of these programs are not mandatory on the States, as commerce clause and Fourteenth Amendment legislation is, but since they require State compliance as a condition of receiving Federal program funds, the effect may be about the same. They are, moreover, the only way that the Federal government can affect the internal management and functioning of a State government where there is no Fourteenth Amendment interest. While the Fourteenth Amendment enables the Federal government to forbid the States to discriminate improperly against individuals, or to deprive them of their Constitutional rights, neither the Fourteenth Amendment nor the commerce clause would seem to enable the Federal government to regulate State activities that are essential to the performance of *internal* governmental

functions, such as record keeping. As recently as 1976, the U.S. Supreme Court ruled in *National League of Cities v. Usery*[1] that the Federal government may not legislate in ways that "operate to directly displace the States' freedom to structure integral operations in areas of traditional governmental functions." The national government, in other words, may not use *coercion* to influence, for example, State government record-keeping practices, but the *National League of Cities* decision does not preclude the use of *inducements*, such as making certain record-keeping practices a condition of Federal funding.

State Protections for Personal Privacy

Within the strictures the Federal government imposes on public and private-sector record-keeping practices, some States have strengthened the federally prescribed protections. California, for example, includes in its State Constitution a specific protection for the "inalienable right" to personal privacy. The California guarantee goes beyond traditional limitations on government surveillance and government access to information to include protections for the records about individuals maintained by private and public entities. The California legislature has followed court interpretations of the State Constitutional provisions and, in specific areas of record keeping, has enacted statutes that prescribe procedures whereby an individual can exercise his right to participate in a record keeper's decision to disclose information about him.

In response to the invitation in the Federal Fair Credit Reporting Act, a number of States have passed their own credit-reporting laws, and some go considerably beyond the strictures of the Federal law, but there is little consistency among State laws to protect records maintained about individuals, in either the scope or the degree of protection provided, and few States give adequate minimal protection.[2]

The States have been active in privacy protection, and in many cases innovative, but neither they nor the Federal government have taken full advantage of each other's experimentation. Altogether, the Commission's inquiry into State record-keeping practices forces it to conclude that an individual today cannot rely on State government to protect his interests in the records and record-keeping practices of either State agencies or private entities.

This is not true, of course, of all States. Some of them approach the protection of the individual's interests in State records and record keeping in as comprehensive a way as has the Federal government. Seven States have enacted omnibus statutes similar to the Privacy Act of 1974 to regulate the collection, maintenance, use, and disclosure of State agency records. The Constitutions of four States provide a right to privacy that includes a record keeper's corresponding duty to keep certain records confidential. Several

[1] *National League of Cities v. Usery* 426 U.S. 833 (1976).

[2] An overview of State efforts and a comprehensive list of State legislation affecting the rights of individuals in records and record-keeping practices will be published separately as an appendix volume to this report.

States regulate the employment and personnel record-keeping practices of their State agencies. Almost every State has some kind of freedom of information or public records law opening State government records to public inspection. The States diverge widely, however, in their determinations of which records belong in the category of public records. Some exempt from disclosure specific categories of records, such as tax and adoption records; others exempt records that are required or permitted by any other statute to be withheld; and still others adopt the Federal standard and prohibit disclosure of information in government records if disclosure would constitute an unwarranted invasion of personal privacy. A few exempt any records if their disclosure would result in a denial of Federal funds, a provision that brings into focus the far-reaching effect of linking privacy protection requirements to the receipt of Federal funding.

Whatever a State may or may not elect to do about its own record-keeping practices, requirements to collect or protect information, or both, flow with Federal money and often supersede whatever State arrangements exist. On another level, the constraints thus placed on State activity frequently require private organizations to alter their record-keeping practices. The information collection criteria established by portions of the Medicaid program, for example, require State agencies to collect and retain information which they gather from private organizations, which, in turn, may very well have to keep certain records, or keep records in certain ways that they would not otherwise do.

State Record-Keeping Practices

The Commission looked at the State's role in protecting personal privacy from two perspectives: the State government as record keeper, and the State as regulator of the record-keeping practices of private organizations. In selecting State public-sector record-keeping relationships to examine, the Commission concentrated on areas in which the Federal government exercises substantial responsibility, and thus looked primarily at the State role as an implementor of national policy. As noted above, the Commission is also aware of the Constitutional limits on the power of the Federal government to regulate the activities of State government that are essential to the performance of internal governmental functions, such as record keeping. For these reasons, most of the recommended measures that directly effect State record-keeping practices can be implemented as a condition of Federal funding under various programs.

The Commission emphatically does not recommend wholesale application by the Federal government of the Privacy Act of 1974 to State and local government record keeping. The Commission believes that the States' creative work in devising privacy protections for the individual in his relationships with State government should continue. Indeed, the Commission believes that the fair information practice statutes or executive orders of the several States that have them constitute one good approach to resolving the privacy protection problems raised by a State's own record-keeping practices. The recommendations advanced in Chapter 9 of this report

regarding government access to records about individuals maintained by private organizations, the recommendations in Chapters 10 and 11, on education and on public assistance and social services record keeping, and the analysis of record-keeping practices and requirements associated with various aspects of the citizen-government relationship in Chapters 13 through 15, should help to guide the States in determining the type, degree, and mode of protections they will provide the individual in their own record-keeping operations.

Furthermore, while the Federal government has placed certain privacy protection requirements on States as a condition of receiving Federal funding, the cut-off of funds is an extreme and rarely effective enforcement technique. Hence, implementing such minimum protections by State law can have two advantages. A State can extend its requirements to the State agencies and organizations that do not receive Federal funds or benefits; and, it can use more flexible enforcement mechanisms and incentives for compliance than termination of Federal benefits. Depriving a State agency of Federal funds, for example, does not help an individual whose rights have been violated, and it harms other individuals. It is seldom an effective incentive for compliance since the sanction is so drastic that the threat of it lacks credibility, especially if the program is a large one where cutting off Federal funds would penalize a great many blameless individuals. By contrast, a State statute can create the alternative of allowing aggrieved individuals to seek redress and remedy against States in State courts, and can provide administrative or criminal sanctions for remiss State employees without disrupting the entire program.

THE STATE ROLE IN A NATIONAL POLICY

In formulating its recommendations, the Commission has recognized and encouraged the existing role of the States in providing individuals with the ability to protect their own interests. In areas such as insurance and medical care, for example, the Commission suggests that the States retain their current power to regulate in conjunction with the creation or extension of a Federal role. Indeed, the significant increase in State regulatory efforts to protect the interests of the individual in records kept about him, noted above, has already led a number of States to try out innovative protections, particularly in their regulation of private-sector organizations. Of the four States that extend Constitutional privacy protections to records about individuals, all apply these same restrictions to their local governments, and two apply them to private organizations as well. Eleven States have gone beyond the protection required by the Federal Fair Credit Reporting Act and enacted Fair Credit Reporting statutes to legislate somewhat stricter requirements. A number of States restrict the disclosure of bank records and define the confidentiality an individual has a right to expect, a right not currently recognized in Federal law for either credit or depository relationships. A number of States have enacted statutes regulating the disclosure of medical records about individuals, many using their licensing

power to enforce this standard of confidentiality. A number of States recognize a patient's right of access to medical records about him.

The Commission takes no single position on the general role of State governments in regulating record-keeping practices. It suggests a role for State agencies in most of the areas it has examined, but always in the context of the current division of regulatory responsibility between the Federal government and the States. The recommended measures create no new authority to regulate the record keeping of organizations that are not now subject to State regulation, nor do they deprive a State of regulatory authority it now has.

Consider, for example, the recommendations regarding credit and depository institutions. The authority to regulate financial institutions is shared between Federal and State governments, and the Federal government has not preempted State regulation. Nonetheless, the recommended measures recognize the ability to preempt certain State regulation and therefore rely on Federal statutes and enforcement mechanisms. Yet, beyond setting basic protection requirements, the recommendations do not limit existing State authority. The States would remain free to provide additional legal protections for the interest of an individual in the records about him maintained by financial institutions.

Or consider the reverse. Regulation of insurance is traditionally the province of the States where the Federal government does not act. As Chapter 5 points out, however, the States have not provided adequate protection for the interests of the individual in the records insurers maintain about him. Thus, the Commission recommends Federal statutes to establish certain basic rights of access and correction, but these protections depend on the individual to assert the rights the Federal statutes would give him, and on State regulatory agencies as well as Federal agencies where the States do not act to provide oversight of insurance company compliance. The State role is defined in several recommendations. The Commission recommends that States amend their unfair trade practices acts, so that they can establish and enforce the recommended notification requirements. The Commission also recommends that State governmental mechanisms receive complaints regarding the propriety of information collected by insurance companies and bring them before policy-making bodies that have the authority to address them, or if the existing entity already has such authority, to consider such propriety questions itself.

In the record-keeping relationships that directly involve State agencies, the Commission recommends that protections for the individual be required as a condition for the receipt of Federal assistance. These areas are: public assistance and social services, education, research and statistical activities, and the confidentiality and use of Federal tax returns. In each of these areas, the extent to which the Commission's recommendations must be implemented thus will depend upon the degree to which the State's agencies participate in the relevant Federal programs. In two of these five areas, moreover—public assistance and social services, and the confidentiality of Federal income tax data—the Commission recommends that States be required to enact prescribed statutes establishing protections for personal

privacy. In both cases, the State agencies themselves are the primary recipients of either money or information from the Federal government, and also, most States have supervisory responsibility for much of the activity conducted by their county and city governments. In public assistance and social services, the Commission further recommends that each State enact a statute that would also apply to public assistance and social service programs in the State that do not receive Federal assistance, although it does not recommend or suggest that the enactment of a statute of that scope be a Federal requirement.

The medical-care area is something of a special case because the State's major role there is to reimburse Medicaid expenses. It is not usually a primary medical-care provider, nor is it involved in the flow of Federal assistance to individuals through the Medicare program where most of the direct Federal requirements on medical-care providers are imposed through the process of qualifying for Medicare participation. Nonetheless, the Commission still recommends that States enact their own statutes incorporating the protections for medical records recommended by the Commission so that individuals will not have to rely on the Federal government to enforce the rights the recommended measures would establish and so that the recommended rights and obligations can be extended to public and private medical-care providers who do not need to qualify for Medicare or Medicaid participation.

In research and statistical activities, Federal assistance usually flows directly to the performing institution through discretionary grants and contracts. The only State agencies that receive an appreciable amount of Federal funding for research and statistical activities are State universities. Chapter 15 presents guidelines for the protection of personal privacy which the Commission recommends as a basis for the research and statistical activities conducted by State agencies or with State assistance.

The Commission's major departure from the general policy of relying on the State to implement Federal requirements is in education. There the Commission does not recommend a State role. Several factors influenced this decision. First, Federal regulation of record-keeping practices under the Family Educational Rights and Privacy Act (FERPA) does not require an implementing State law, mainly because most Federal funds flow directly to local school districts or to universities. The recommended measures strengthen FERPA protections but do not alter that process. Second, the Federal law is comprehensive, and since almost every public and private educational institution currently receives Federal assistance, State law would not extend the law's coverage appreciably. Third, although there are State educational codes for public elementary and secondary schools, those schools have a strong tradition of local autonomy.

Nonetheless, nothing in current FERPA provisions or in the Commission's recommendations prevents a State from enacting its own legislation as long as the Federal requirements are met. Indeed, California, for one, has already done so, and the protections prescribed by California law are stricter than FERPA's. But while State law may be needed to provide civil remedies for individuals whose rights with respect to education records are violated,

the Commission prefers to stress local accountability in education as in the other areas. The recommended provisions of recourse to a Federal court which could enjoin the institution to respect the individual's FERPA rights should provide a vehicle for redress of grievances, if and when a governing board fails to see that an educational institution discharges its obligations to an individual.

It should be noted that in all of these areas, in addition to keeping the privacy protections required of State agencies to the minimum, most of the recommended measures leave the primary responsibility for enforcement with the States, seeking to strengthen the accountability of State agencies to their State legislatures and courts rather than making them more accountable to the Federal government. Concomitantly, the recommended measures restrict the Federal role to first reviewing and approving the required State law or policy, and then to receiving complaints about State enforcement efforts. Moreover, the Commission relies wherever possible on existing mechanisms to monitor performance: in medicine, the Joint Commission on Accreditation of Hospitals and State licensing agencies; in research and statistical activities, institutional review boards; in public assistance and social services, appropriate State agencies; and in education, elected boards and institutional governing boards.

In the matter of Federal sanctions, the Commission concluded that a Federal agency should have some alternative sanctions short of cutting off all Federal funds when a State or private agency is in violation. These alternatives might include withholding or asking for the return of a proportion of benefits, graduated according to the seriousness of the violation. In categorical grant programs a percentage of the total grant could be withdrawn as a penalty or withheld as security for specific performance of obligations. In reimbursement programs, monies could be withheld on a similar basis. To give the Federal agency graduated alternatives would make the threat of sanction credible, which in turn would increase the State's incentive to maintain compliance.

Finally, in a sixth area, employment and personnel, five of the Commission's recommendations specifically affect State employment and personnel record-keeping practices. These recommendations (*Recommendations (6), (7), (8), (9)* and *(10)* in Chapter 6), deal with the use of arrest records in employment. *Recommendations (6), (7)* and *(8)* invite State legislatures to restrict State use of arrest records in determining eligibility for employment and licensing. *Recommendation (9)* further expresses the Commission's deep mistrust of the use of arrest records in employment by recommending Federal financial assistance to States to help them devise means of limiting inappropriate arrest disclosures to employers by State and local law enforcement agencies, and to improve the accuracy and timeliness of arrest records.

As noted earlier, the Commission does not recommend that State governments be required to adopt a particular omnibus privacy protection statute to regulate their agencies' record keeping. The Privacy Act, however, recognizes that the Federal government owes the States assistance in developing appropriate legislation. In fact, the Privacy Act authorized the

Commission to provide technical assistance in the preparation and implementation of such legislation. The Commission sees a clear need for continued assistance of this kind, and includes suggestions to this effect in the chapters on medical records, education, and public assistance, and also in the implementation discussion in Chapter 1.

With respect to records maintained or regulated by State agencies, the Commission also makes two quite specific recommendations: (1) that States amend their penal codes to provide criminal penalties for getting information from a medical-care provider through deception or misrepresentation; and (2) that each State review all direct-mail marketing and solicitation uses made of State records about individuals. This is especially important when State agencies prepare mailing lists for the express purpose of publishing, selling, or exchanging them, as motor vehicle departments often do without apprising drivers and owners of registered vehicles that they do so. The Commission recommends that State agencies be directed to develop a procedure whereby an individual can notify the agency and, through the agency, any user of the record for direct mail marketing or solicitation that he does not want his name disclosed for such a purpose.

State Agency Access to Third-Party Records

For many of the record-keeping relationships examined in this report, the Commission recommends constraining the voluntary disclosure of records about an individual by private-sector record keepers. Individually identifiable credit, depository, and insurance records may not be disclosed without the authority of the individual to whom they pertain or the presentation of valid compulsory legal process. This would include disclosures to State and local government agencies. There are exceptions, of course, where valid legal process is served on the record keeper or where the record keeper is subject to statutory reporting requirements. With respect to the use of Federal tax return information, the recommended measures also prohibit any disclosure by one State agency to another for nontax purposes. With respect to federally assisted research or statistical projects, no recorded information may be disclosed in individually identifiable form for any purpose other than a research or statistical purpose or the purpose of auditing a grant or contract.

To the extent that these restrictions affect State agencies, they place few specific limitations on State use of compulsory legal process or even on State reporting requirements. The limitations on Federal compulsory processes and Federal reporting statutes recommended in Chapter 9, however, provide a model for the States. Indeed, as noted at several points in that chapter, the broad public policy and specific recommendations it presents are equally applicable to State and local governments. The recommendations were not explicitly directed to the States because of the difficulties of dealing properly with fine, but often crucial, distinctions in the forms of compulsory legal process in 50 jurisdictions.

Chapter 13

The Relationship Between Citizen and Government: The Privacy Act of 1974

The Privacy Protection Study Commission was given the broad mandate to investigate the personal-data record-keeping practices of governmental, regional, and private organizations and to recommend to the President and the Congress the extent, if any, to which the principles and requirements of the Act should be applied to them.[1] Early in its inquiry, the Commission decided that to fulfill this mandate an assessment of the Privacy Act itself, its underlying philosophy, and the experience of Federal agencies to date in complying with it would be necessary. This chapter reports the results of that assessment. In so doing, it responds to the Commission's mandate directing it to:

> report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information. *[Section 5(b)(2) of Public Law 93-579]*

As the preceding chapters demonstrate, the Commission has concluded that the Privacy Act should *not* be extended in its present form to organizations outside the Federal government. This conclusion is based on several considerations. First, economic incentives can be used to induce organizations in the private sector to limit their acquisition and retention of information about individuals much more easily than they can be used in government. Private-sector organizations can be moved to protect their customers' privacy interests if their customers know and understand their record-keeping practices and use the competition of the marketplace as an ally in securing compliance with privacy protection safeguards. In addition, a private-sector organization's legal liability for violation of certain individual rights compels attention to fair practices and procedures in carrying out privacy protection safeguards even at the lowest levels. A mistake that costs a company money can cost the responsible employee his job. In government organizations, however, such incentives are much more tenuous, as the discussion later in this chapter will indicate.

A second consideration that argues for distinguishing private organizations from governmental ones is the high degree of uniformity, particular-

[1] Section 5(b)(1) of Public Law 93-579.

ly of Federal government administrative processes and practices, in contrast to the diversity of similar practices found at other levels of government and throughout the private sector. The standards of government operation outlined in the Administrative Procedures Act *[5 U.S.C. 551 et seq.]* apply to all but the most limited of Federal agency activities. No parallel exists in the private sector.

The third consideration that led the Commission to reject wholesale, uniform application of the Privacy Act to other than Federal government agencies is related to the second; uniform and specific Federal requirements imposed on all private-sector record keepers and other governmental ones would inevitably require broad-based regulation, giving government an unprecedented role in channeling and monitoring flows of information throughout all of society. While the Commission recognizes that government intervention in some areas of record keeping may not be avoidable, it strongly believes that the safeguards for personal privacy it seeks to establish and preserve require and, in fact, demand that such intervention be limited and controlled.

A fourth reason for concluding that the Privacy Act should not be extended to organizations outside the Federal government is the recognition that some of the requirements imposed by the Privacy Act on Federal agencies simply do not, or cannot, apply to private-sector organizations. For example, the restriction the Privacy Act places on the collection of information on an individual's exercise of his First Amendment rights would be ill-considered, and perhaps unconstitutional, if it were to be applied to all private-sector organizations without limitation.

Finally, the Commission has reached the conclusion that the Privacy Act needs significant modification and change if it is to accomplish its objectives within the Federal government. Much of this chapter supports that conclusion.

All of these arguments persuaded the Commission that it should not recommend omnibus legislation to extend the Privacy Act to other levels of government or to the private sector. The Commission further observes that even within the Federal government different requirements apply to some records about individuals. While the Privacy Act establishes minimum requirements for the keeping of records about individuals, other statutes set out additional ones directed at records maintained by particular agencies or used to perform particular functions.

The prohibitions on the disclosure of individual tax returns in the Tax Reform Act of 1976 are one example of such legislation. The rationale for these additional requirements recognizes that in government information about individuals is often acquired and recorded under different circumstances by different agencies. While every individual has a basic relationship with government that demands a minimum set of protections against abuse of the records government keeps about him, in specific circumstances the individual is entitled to a higher threshold of protection. This is particularly true in relation to standards limiting disclosure. The information a citizen gives to the revenue system, for example, because he is forced to do so under the threat of criminal sanctions, deserves more than minimum protections.

The Commission, as further discussed in Chapter 14, encourages the Congress to enact specifically targeted legislation in areas where the amount of detail in the records, the manner in which they are obtained, or the nature of the agency mission involved, warrant special safeguards.

METHOD OF STUDY AND ANALYSIS

To assess the Privacy Act's requirements and the effectiveness of its implementation, the Commission sought to identify the principles and underlying philosophy that formed the basis for the Act. To do so, a study of the Act's legislative history, the language of the law, and its actual implementation was necessary. The findings and conclusions presented below are based on communications with agency heads and their designated Privacy Act points-of-contact, testimony from various Commission hearings, agency annual reports, some informal workshops, and literally hundreds of personal and telephone interviews by staff. Although the Commission's inquiry was conducted in the early days of the Act's implementation, it believes that this close and continuous staff contact with agency operating personnel has allowed a fair assessment of agency implementation experience.[2]

In conducting its inquiry, however, the Commission encountered both conceptual and drafting problems with the current law. As the subsequent discussion will indicate, drafting details can have important consequences in an area which is both new to regulation and dependent upon changing technology. Thus, the Commission's conclusions concentrate on policy objectives rather than on the specifics of implementation. Its objective in setting out its conclusions and offering suggestions for change in the Act is to allow the policy objectives of the current law to be achieved more successfully without destroying necessary opportunities for flexibility in implementation. The Commission adopted this approach to allow for changing information technology and diversity of agency information needs and uses, as well as to foster the constructive creativity that can arise in the absence of overly restrictive requirements.

In many instances, the difficulty with the current law is not in its objectives nor in the flexibility it allows, but rather that agencies have taken advantage of its flexibility to contravene its spirit. Yet, making the law less flexible is not a desirable solution. Implementation costs would rise dramatically, and new developments in information technology could invite uncontrollable circumvention of rigidities in the statute. Thus, the Commission's approach is to strengthen flexibility and provide incentives for agency compliance while preserving the essential autonomy of each agency to decide how best to comply with each requirement.

If one accepts the view that it is best to tell an agency *what* to do, rather than *how* to do it, there are still issues that each agency cannot, and in some cases should not, resolve singly. The most obvious one is the question of

[2] The detailed results of this inquiry will be presented in a separately published appendix volume that will also contain an illustrative statute showing how the Commission's suggestions might appear as legislative requirements.

whether a particular type of record-keeping system should exist at all; another is whether particular transfers of records among agencies are desirable. Such questions require independent policy judgments and thus must be addressed by an entity other than the one directly involved. In Chapter 1, the Commission enumerates the functions it believes such an entity should fulfill.

Finally, it is worth noting at the outset that the concerns expressed by the various agencies at the time of the Act's passage regarding anticipated costs of implementation, numbers of access requests, and burden of administration have generally proved to be unwarranted. For example, the expected controversy over patient access to medical records has not developed. Cost figures recently released by the Office of Management and Budget (OMB) show expenditures to be much lower than originally estimated. In 1974, OMB had estimated that implementing the Act would cost $200-$300 million per year over the first four to five years and require an additional one time start-up cost of $100 million, which would be expended in the first two years. In 1977, however, OMB estimated that start-up costs in the nine months between the Act's passage and the date it took effect were $29,459,000, and that an additional $36,599,000 was spent for first-year operating expenses.[3]

The Privacy Act Principles

The *requirements* of an act, although not always easy to interpret, derive from the words of legislation. *Principles,* on the other hand, are sometimes less readily apparent. The statement of principles in a law's preamble, the law's legislative history, and the conditions or problems that led to its passage must all be read along with the language of its specific provisions.

Although many issues in the 1960's and early 1970's were loosely grouped under the category of invasions of privacy, it is clear that many of the perceived problems had very little in common. Some of the actual or potential invasions of privacy involved physical surveillance or wiretapping; some involved mail openings or burglaries conducted by government agencies; others centered on harassment of individuals for political purposes; and still others concerned the unfair use of records about individuals.

The inquiry into these matters by a number of congressional committees did not share a common analytical framework, nor were the distinctions among different types of privacy invasions sharply drawn. Nonetheless, they succeeded in focusing public attention on privacy issues and in amassing useful information regarding particular aspects of the privacy protection problem.

In 1972, the Secretary's Advisory Committee on Automated Personal Data Systems was appointed by the then Secretary of Health, Education,

[3] Letter from Hon. Bert Lance, Director, Office of Management and Budget, to Senator Abraham A. Ribicoff, Chairman, Committee on Governmental Affairs, United States Senate, March, 1977, including a report on Costs of Implementing the Privacy Act of 1974, p. 5.

and Welfare, Elliot L. Richardson, to explore, as its name suggested, the impact of computers on record keeping about individuals and, in addition, to inquire into, and make recommendations regarding, the use of the Social Security number. The Advisory Committee did not examine issues arising from the physical surveillance of individuals or the wiretapping of conversations. Nor did it study mail openings, harassment of political dissidents, or violations of Fourth or Fifth Amendments rights. Instead, the Committee limited its inquiry to the use of records about individuals by government agencies and private organizations, and it focused its recommendations on automated systems while also suggesting their possible applicability to manual systems.

After examining various definitions of privacy, the Secretary's Advisory Committee concluded that the most significant aspect of the way organizations keep and use records about individuals was the extent to which individuals to whom the records pertained were unable to control their use. Accordingly, to strike a better balance between institutional and individual prerogatives, the Committee recommended a "Code of Fair Information Practices" based on the following five principles:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[4]

These five principles and the findings of the DHEW Committee, published in July 1973, are generally credited with supplying the intellectual framework for the Privacy Act of 1974, though in drafting the statute the Congress, influenced by its own inquiries, refined the five principles to eight:[5]

(1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems. (The Openness Principle)

(2) An individual about whom information is maintained by a record-keeping organization in individually identifiable form

[4] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, (Washington: U.S. Government Printing Office, 1973), p. 41.

[5] This identification of eight principles results from Commission analysis, not a specific Congressional statement.

shall have a right to see and copy that information. (The Individual Access Principle)

(3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle)

(4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle)

(5) There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle)

(6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle)

(7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate. (The Information Management Principle)

(8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle)

Each of these principles is manifest in one or more of the Privacy Act's specific requirements, and in their application they all require a balancing of individual, organizational, and societal interests.

FINDINGS AND CONCLUSIONS

In assessing the Privacy Act of 1974, the Commission sought answers to the following two questions:

- Does the Act effectively address the issues and problems it was intended to address?
- Are there important information policy issues and problems the Act might address but does not address, or does not address adequately?

On the whole, the Commission has concluded that:

(1) The Privacy Act represents a large step forward, but it has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect;

(2) Agency compliance with the Act is difficult to assess because of

the ambiguity of some of the Act's requirements, but, on balance, it appears to be neither deplorable nor exemplary;

(3) The Act ignores or only marginally addresses some personal-data record-keeping policy issues of major importance now and for the future.

The more specific conclusions that follow stem from these three basic conclusions. The Commission believes that if the Congress seeks to remedy these deficiencies by amending the Act, three steps are essential:

First, the ambiguous language in the law should be clarified to minimize variations in interpretation, but not implementation, of the law.

Second, any clarification should incorporate "reasonableness tests" to allow flexibility and thus give the agencies incentives to attend to implementation issues and to take account of the differences between manual and automated record keeping, diverse agency record-keeping requirements, and future technological developments.

Third, the Act's reliance on its system-of-records definition as the sole basis for activating all of its requirements should be abandoned in favor of an approach that activates specific requirements as warranted.

The impact of the first two of these suggestions will become clear when the specifics of the Commission's other, more detailed, conclusions are explained. The third, however, is central to the operation of the Act. From an examination of both the language of the Act and its legislative history, it seems clear that the intent of Congress was to include in the definition of the term "record"[6] every one that contains *any* kind of individually identifiable information about an individual. However, because the Congress was mindful of the burden such a definition could impose on an agency, it limited the Act's coverage to records retrieved from a "system of records" by "name . . . or identifying number, symbol, or other identifying particular . . . ." *[5 U.S.C. 552a(a)(5)]* Thus, unless an agency, in fact, retrieves recorded information by reference to a "name . . . identifying symbol, or other identifying particular . . .," the system in which the information is maintained is not covered by the Act. Whereas the current record definition refers to information about an individual which *contains* his name or identifier, the system-of-records definition refers to information about an individual which is *retrieved* by name, identifier, or identifying particular. The crucial difference is obvious, and the effect has been wholesale exclusion from the Act's scope of records that are not accessed by name,

[6] The Act defines a "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *[5 U.S.C. 552a(a)(4)]*

identifier, or assigned particular. None of the Act's protections accrue to an individual whose record is so treated.

There are many examples of readily accessible individually identifiable agency records that are not retrieved by personal identifier,[7] and current and emerging computer and telecommunications technology will create more. While the language of the Act speaks in terms of retrieval by discrete individual identifiers, most automated record systems facilitate identification of an individual's record based on some combination of the individual's attributes or characteristics, natural or assigned, as well as by reference to individual identifiers in the more conventional sense. Thus, it would be easy to program a computer to locate particular individuals through attribute searches (e.g., "list all blonde, female Executive Directors of Federal Commissions").[8] Retrieval of individually identifiable information by scanning (or searching) large volumes of computer records is not only possible but an ever-increasing agency practice. The Federal Trade Commission, for example, is transcribing all written material in its litigation files for computer retrieval, thereby making it possible to search for all occurrences of a particular name, or any other character pattern for that matter.

In summary, the system-of-records definition has two limitations. First, it undermines the Act's objective of allowing an individual to have access to the records an agency maintains about him, and second, by serving as the activating, or "on/off switch" for the Act's other provisions, it unnecessarily limits the Act's scope. To solve this problem without placing an unreasonable burden on the agencies, the Commission believes *the Act's definition of a system of records should be abandoned and its definition of a record amended.*

The term *record* should include attributes and other personal characteristics assigned to an individual, and a new term, *accessible record,* should be defined to delineate those individually identifiable records that ought to be available to an individual in response to an access request. Accessible records would include those which, while not retrieved by an individual identifier, could be retrieved by an agency without unreasonably burdening it, either through its regular retrieval procedures or because the subject is able to help the agency find the record. If an individual knew he was mentioned in a particular record, for example, he would be entitled to access to it whether or not agency practice is to access the record by reference to him.

The Commission believes that *when an individual asks to see and copy information an agency maintains on him, the agency should be required to*

[7] Two examples will illustrate the extremes of agency implementation of the "system of records" provision. A small component of one agency rearranged its personnel records by Civil Service grade, instead of individual identifier, in order to avoid the Act's requirements. The Department of the Navy, on the other hand, elected to bring a file of interview records under the Act even though they were filed (and hence retrieved) by the date of the interview.

[8] An "attribute search," contrary to the more common "name search," or "index search," starts with a collection of data about many individuals and seeks to identify those particular individuals in the system who meet the prescribed conditions or who have the prescribed attributes.

provide that information if it can do so without an unreasonable expenditure of time, money, or other resources or if the individual can provide specific enough locating information to render the record accessible without an unreasonable expenditure. In implementing this provision, however, an agency should not have to establish any new cross-referencing schemes for the purpose of granting access, such as would be required if the agency had to be aware of all references to one individual in other individuals' files or in files indexed in any other manner (e.g., references to agency officers in files indexed by agency name). In this connection, the Commission would also urge deletion of the clause (in Subsection d(1)) of the Act which requires an agency to allow an individual access "to any information pertaining to him which is contained in the system . . . ." This requirement is impossible to satisfy since an agency often does not know how to find "all" such information.

The Commission also believes that the terms *record, individually identifiable record,* and *accessible record* should operate as separate activators, or "on/off switches," for the appropriate provisions of the Act. For example, the Act's civil remedies could apply in all cases in which the misuse of an individually identifiable record through failure to comply with one of the Act's requirements resulted in injury to an individual, while the access to records provision could be subject to the reasonable burden test of the accessible record definition. This would allow more flexibility and broaden the scope of the current Act.

Another provision of the Act that limits its scope is the one dealing with contractors. Recipients of discretionary Federal grants who perform functions similar or identical to functions performed by contractors are not covered. Agency personnel interviewed by Commission staff frequently expressed the view that the implicit distinction in the Act between contractors and grantees is, in many cases, artificial. The Commission agrees. In Chapter 15, moreover, it recommends that a uniform set of requirements and safeguards be applied to records collected or maintained in individually identifiable form for a research or statistical purpose under Federal authority or with Federal funds, and the Privacy Act is suggested as a basic vehicle for implementing these recommendations.

While care must be taken to avoid creating undue burdens on the contractor or grantee, the Commission believes that *the Federal government must assure that the basic protections of the Privacy Act apply to records generated with Federal funds for use by the Federal government.* Specifically, the Commission believes that any contractor or recipient of a discretionary Federal grant, or any subcontractor thereof, who performs any function on behalf of a Federal agency which requires the contractor or grantee to maintain individually identifiable records, should be subject to the provisions of the Act. The Act, however, should not apply to employment, personnel, or administrative records the contractor or grantee maintains as a necessary aspect of supporting the contract or grant, but which bear no other relation to its performance. The Act also should not apply to individually identifiable records to which the following three conditions all apply: (1) records that are neither required nor implied by terms of the contract or grant; (2) records for which no representation of Federal

sponsorship or association is made; and (3) records that will not be provided to the Federal agency with which the contract or grant is established, except for authorized audits or investigations. The added specificity in delineating which records fall within the Act's purview represents an attempt to preserve the intent of the Act while removing some of the confusion that could result in undue burden on contractors and grantees.

The remaining analysis of agency implementation of the Privacy Act will be based on the eight Privacy Act principles identified earlier. The extent of their fulfillment will be examined and the Commission's suggestions for change in their implementation will be presented and explained.

Implementation of the Privacy Act Principles

The Openness Principle

The Privacy Act asserts that an agency of the Federal government must not be secretive about its personal-data record-keeping policies, practices, and systems. No agency may conceal the existence of any personal-data record-keeping system, and each agency that maintains such a system must describe publicly both the kinds of information in it and the manner in which it will be used. This is accomplished in two ways. The first is through the required annual publication of system notices in the *Federal Register*. The second is through the "Privacy Act Statement"[9] given at the time individually identifiable information is collected from an individual.

The requirements implementing the Openness Principle are intended to achieve two general goals:

(1) facilitate public scrutiny of Federal agency record-keeping policies, practices, and systems by interested and knowledgeable parties; and
(2) make the citizen aware of systems in which a record on him is likely to exist.

The Commission has found that the Act has made a significant step toward fulfillment of these objectives, especially the first one, but that it has still fallen short of expectations.

The Commission believes that publishing record-system notices once each year in the *Federal Register* is worthwhile. It develops an inventory of agency record-keeping operations that is useful for both public scrutiny of Federal agency record-keeping practices and for internal management control. Unfortunately, however, the annual notices tend to be less informative than they could be, and they are not required to describe the extent to which information is used within the agency. Furthermore, the Act is silent on the distinction between a *system* and a *subsystem*, and there are no criteria for limiting the diversity of information, purposes, or functions that may be incorporated in any one record system, and thus subsumed in

[9] The "Privacy Act Statement" contains the authority for the solicitation of the information, the principal purposes for which it will be used, its "routine uses," and the effect on the individual of not providing the information. *[5 U.S.C. 552a(e)(3)]*

one annual *Federal Register* notice. As a result, some annual notices are too encompassing to be informative. Likewise, duplicate, substantially similar, or derivative systems are frequently either unlisted or not cross-referenced. The Commission believes that the primary purpose of the public notice requirement should be to facilitate internal and external oversight of agency activities, including public scrutiny. Thus, it believes that *the annual notices should provide more detail than they now do and should reflect more accurately the context or manner in which an agency maintains records.*

One of the specific shortcomings of the system notices has been the literal interpretation of the requirement to describe the *routine uses.* While limiting these descriptions to *external* uses is consistent with the prevailing interpretation of the Act's routine-use definition, in many cases, the more significant uses are *internal* ones. Therefore, the Commission believes that *the section in the annual notice on routine uses of records maintained in a system, including categories of uses and the purposes of such uses, should include a description of internal uses of information as well as external disclosures.*

Describing the context and manner in which an agency uses the records in a system would at least partially reveal the relationships among systems that are often obscured today. When a large, complex record system is covered by one system notice, the subsystems should be described in detail. The important concern should not be to define the level at which a subsystem must be described, or the way to describe indices, but rather that an agency present a true picture of how it uses information in a system and how the system itself is perceived by the agency. The goal should be to remain faithful to the Openness Principle by assuring that there are no secret systems. The possibility that an agency may comply with the technical requirements of the Act's notice provisions but still maintain systems that are effectively secret must be avoided.

The goal of facilitating public scrutiny is hindered by the fact that the *Federal Register* is at best a limited vehicle for reaching the general public. Every effort should be made to classify, compile, and index the information in notices logically. For example, it would be useful to differentiate between the large group of systems that are solely devoted to record keeping about agency personnel and the much smaller group that contains information on citizens in general. The *Federal Register* compilation should make it easy for a private citizen, a member of a public interest group, or a congressional staff member to pinpoint a particular type of record or system of records.

Given the limited readership of the *Federal Register*, however, the best way of making the citizen aware of systems in which he is included is through the "Privacy Act Statement," which is similar to the annual system notice, except that it also informs the individual of internal agency uses of information about him. Like the annual notices, however, Privacy Act Statements are often too vague or general to inform the individual adequately. They need not explain that supplementary information may be collected from other sources and not every agency or system is subject to the Statement requirement.

There is a problem in finding a balance between the length of a Privacy Act Statement and its clarity; if it is too long, individuals are not

likely to read it; if it is too short, it may not convey enough information for the individual to understand fully how the information will be used. The contents of the Privacy Act Statement are discussed in the section on the Collection Limitation Principle.

The Individual Access Principle

The Privacy Act's second principle is that an individual should have a right to see and obtain a copy of a record an agency maintains about him. Prior to the Act's passage, an individual was able to obtain copies of the records a Federal agency might keep about him in several ways. The Armed Services, for example, made many personnel, medical, and performance records available to servicemen. In fact, the subjects of certain personnel records are required to review and sign them once each year. Federal agencies also have procedures that give an individual access to records about him when there is a dispute over his entitlement to benefits.

In addition, the Freedom of Information Act (FOIA) *[5 U.S.C. 552]*, which predates the Privacy Act by seven years, allows any person to see and obtain a copy of any record in the possession of the Federal government without regard to his need for or interest in it. An agency can withhold a record that falls within one of nine FOIA exemptions, but its determination to do so, if appealed by the requestor, must withstand administrative and judicial review.

Individuals could and did use the Freedom of Information Act to gain access to their own files prior to passage of the Privacy Act. There were several drawbacks, however. First, an agency could decline to release information deemed to be part of the internal deliberative processes of government.[10] In certain cases, this resulted in a considerable amount of information about an individual being taken out of a file prior to giving the file to him. Second, in the early days of the Freedom of Information Act, some agencies refused to disclose personnel and medical files to an individual on the grounds that disclosure to the individual would constitute a clearly unwarranted invasion of *his* personal privacy.[11]

The individual access provision of the Privacy Act *[5 U.S.C. 552a(d)]* was enacted in part to clarify these uncertainties with respect to an individual's right to see and obtain a copy of a record about himself. The Privacy Act has its own set of exemptions from its individual access requirement which will be discussed below. For all other systems subject to the Act, however, agencies must now facilitate access by an individual when he so requests and may never keep records about himself from him on the grounds that they constitute communications within or among agencies. Nonetheless, the Commission has found that the number of Privacy Act access requests (i.e., requests specifically citing the Privacy Act) has not been great and that most have come from agency employees or former employees. One reason for this may be that pre-existing law and practice continue to be used. In addition, the public's awareness of the Freedom of

[10] 5 U.S.C. 552(b)(5)
[11] 5 U.S.C. 552(b)(6)

Information Act still appears to be much sharper than its awareness of the Privacy Act. Another reason may also be that the Privacy Act's own exemptions from the access requirement are too sweeping. The Central Intelligence Agency and some major law enforcement systems qualify for a blanket exemption from the access requirement. Thus, individuals who want access to records about themselves in those systems must use the Freedom of Information Act as their vehicle.

The Privacy Act exemptions from the individual access requirement are permissive, not mandatory. In addition, unlike the Freedom of Information Act exemptions, they apply to *systems of records* rather than to *specific requests* for access to specific information. To invoke any one of them an agency must publish its intention to do so in advance. As a result, some over-cautious lawyers and administrators have made excessively broad claims of exemption. Once an exemption is published, moreover, agency operating personnel are inclined to use it, thus eliminating exercises of judgment in light of the particular record sought.

On the other hand, some agencies have not claimed exemptions to which they may have been entitled, and others have claimed them but do not use them. The Central Intelligence Agency, for example, processes individual access requests under the Privacy Act despite having claimed the broad exemption the Act provides it. On balance, however, the Act's requirement that exemptions be claimed in advance, and that they cover entire systems rather than types of records or specific requests, has resulted in unnecessary exclusions of records from the scope of the Act's individual access requirement.

Agency rules on individual access, and on the exercise of the other rights the Act establishes, appear, in most instances, to be in compliance with the Act's rule-making requirements. Yet, they too are often difficult to comprehend, and because the principal places to find them are in the *Federal Register* and the *Code of Federal Regulations*, it is doubtful that many people know they exist, let alone how to locate and interpret them. Furthermore, the Act's requirement that an individual specifically name the record system in which the record he desires is located is not realistic. Fortunately, many agencies have gone beyond the letter of the law in assisting individuals whose access requests reasonably describe the records sought, but the requirement to name the system still seems likely to discourage some people from asking to see their records. Finally, the Act's requirement that an agency keep an accounting of each disclosure of a record to the individual to whom it pertains appears to be an added incentive to process access requests under the Freedom of Information Act rather than the Privacy Act when an agency has a choice (i.e., when the individual does not specify that his request is being made under one Act or the other).

It would appear, in sum, that individuals continue to rely on pre-existing laws and practices when they want access to agency records about themselves. From the individual's point of view, one advantage of the Freedom of Information Act is that there are specific limits on how long an agency may take to respond to a request, whereas in the Privacy Act there

are none. Furthermore, although the FOIA permits agencies to charge search fees, while the Privacy Act does not, in practice such charges are rarely made when an individual is asking for information about himself.

The Privacy Act has benefitted a current or past Federal employee to the extent that it allows him to circumvent the FOIA exemption for documents pertaining to internal agency deliberations when he wants access to some of the more interesting parts of an evaluation report or inquiry into his background. The Privacy Act has retained a limited exemption for some personnel evaluations, but its net effect has been to increase the accessibility of such material. It could also be concluded that Federal employees, unlike the private citizen, are aware that the Act exists and, being comfortable with bureaucratic procedures, have quickly learned how to use it.

To aid an individual in gaining access to his record, the Commission believes that *the Privacy Act should parallel the approach of the Freedom of Information Act in that an individual should be required to make a request which reasonably describes the record to which he desires access.* In those situations in which an agency believes an individual has made too broad an access request, it should help him refine his request. This is the procedure most agencies are following now, but modification of the language of the Act is important. The likelihood of a private citizen being aware of the name of a system of records published in the *Federal Register* is too remote to be relied on.

In addition, the Commission believes that the Privacy Act should be the exclusive vehicle for individuals requesting access to records about themselves, *provided that the Privacy Act's approach to exemptions from the individual access requirement is modified to parallel that of the Freedom of Information Act* (as discussed below). Making the exemption approaches parallel is necessary to assure that the individual does not receive less information using the Privacy Act as his access vehicle than he would if his request for access were processed under the Freedom of Information Act. Because agencies may currently ignore the time limits suggested in guidelines for implementation of the Privacy Act issued by the Office of Management and Budget,[12] *explicit time limits should also be added to the Privacy Act so that by making the Act the individual's exclusive access vehicle he will not lose the time limit protections now in the Freedom of Information Act.* The fees, appeal rights, and sanctions of the Privacy Act, however, would still apply.

Besides the direct benefits for the individual of such an approach there are certain procedural benefits to the agencies which should be noted. Currently, Freedom of Information Act offices and officers are required to respond to requests for access to both personal information about individuals and information about agency activities (e.g., regarding agency policies). By making the Privacy Act the exclusive access vehicle for any individual requesting information about himself, some stress will be removed. The actual number of requests for information will not be affected, but this approach better divides responsibility in the agencies.

[12] Office of Management and Budget, *Privacy Act Guidelines*, issued as a supplement to Circular A-108, *Federal Register*, Volume 40, Number 132, July 9, 1975, pp. 28948 - 28978.

Perhaps some of the confusion surrounding the interrelation between the Freedom of Information Act and the Privacy Act will even be reduced.

In addition to requiring an agency to assist an individual in reasonably describing the records to which he seeks access, it is important for an individual to have access to, and the right to amend, information about which he may not have enough detailed knowledge to formulate a specific request. Thus, the Commission believes that *access to substantially similar or derivative versions of records sought by an individual should be provided automatically in response to his request for the original record to the extent that providing such access does not constitute an unreasonable burden on the agency.*

There are two related situations at issue here. The first is where there may be an exact duplicate of a record maintained in another part of the agency. The second, and more important, is where some portion of a record may have been copied and then subsequently amended, appended, or otherwise altered. Alternatively, two records, or portions thereof, may have been combined. In each of these cases, it can be reasonably inferred that the individual would want to know about all versions of the record were he aware of them. Thus, the burden must be on the agency to take reasonable affirmative steps to describe and, if requested, to make available to the individual the several versions. While the individual may not want to see an exact duplicate of the original record, for example, he may wish to amend it if he amends the original. Moreover, the uses and disclosures of exact duplicates of a record, as well as substantially similar or derivative versions of the record, often will not be the same as the uses and disclosures of the original, and thus it can be assumed that the individual will want to know about them.

The Commission believes that *the Privacy Act's approach to exemptions from the individual access requirement should be modified to parallel that of the Freedom of Information Act.* Currently, Privacy Act exemptions are claimed in advance and apply to entire systems of records. Pre-claimed exemptions can be waived on a case-by-case basis, and while there is evidence that agencies are not using all of the exemptions claimed, they still seem to be claiming every one possible (including, in some cases, exemptions to which they would not appear to be entitled), but then using them only as needed. This creates uncertainty for the individual which the framers of the Act did not intend.

Abandonment of the system-of-records definition currently in the Privacy Act necessitates a different exemption strategy than the one the Act now has. The natural model to use is the Freedom of Information Act. The FOIA allows exemptions for certain types of information rather than for entire systems of records; exemptions may be invoked only when applicable, not claimed in advance. In addition, any segregable portion of a record which by itself does not qualify for an exemption must be provided to the individual. The FOIA approach appears to be working well, and its presumption that access should be granted to any part of a record for which an agency cannot sustain an exemption claim seems highly desirable.

Using the FOIA approach to exemptions would have the unintended effect, however, of voiding the Privacy Act provision that allows the CIA

and law enforcement agencies to maintain unverified information obtained from intelligence or investigative sources.[13] Consequently, if the suggested exemption policy is adopted, it should allow the CIA, or any agency or component thereof which performs as its principal function any activity relating to the enforcement of criminal laws, to maintain information whose accuracy, timeliness, completeness, or relevance is questionable, *provided, however, that such information is clearly identified as such to all users or recipients of it.* This would preserve the Act's current policy. The only new requirement would be that the unverified information be clearly identified as such when it is disclosed to anyone else.

The Commission believes that *certain of the specific exemptions in the Freedom of Information Act should actually be duplicated in the Privacy Act. These include the Freedom of Information Act exemptions dealing with information specifically authorized to be kept secret in the interest of national defense and foreign policy, certain investigative information compiled for law enforcement purposes, and operating reports used by an agency responsible for the supervision of financial institutions.* This, too, would clarify, without altering current policy, and it would have the further advantage of incorporating the existing body of judicial interpretation as to what may or may not be withheld pursuant to the FOIA exemptions. Today, an individual is supposed to be granted access to the larger of the amounts of information to which he would be entitled under the FOIA *or* the Privacy Act, so there seems to be no practical reason for the two Acts to have different exemptions in the same area.

Finally, the Commission believes that *the Act's requirements with respect to a patient's access to a medical record an agency maintains about him should be brought into line with* Recommendation (5) *in Chapter 7 of this report.* The Commission also believes that *the Act should be refined to allow agencies to deny access to a parent or legal guardian in those situations in which another statute authorizes such withholding.*

The Individual Participation Principle

The third Privacy Act principle holds that an individual should have the right to challenge the contents of a record on the grounds that it is not accurate, timely, complete, or relevant. The principle specifically recognizes that information can be a source of unfairness to an individual. In theory, the right to participate in the maintenance of a record allows for complaint, involvement, and representation in order to force a balancing of the individual's interests against the record keeper's. If this principle is enforced, the individual is able to keep some measure of control (although not absolute control) over the substance of what he himself reveals to an agency, as well as to check on what the agency collects about him from other sources.

The Act has made significant progress toward fulfillment of this principle through its requirement that agencies establish procedures whereby the individual may request correction or amendment of a record,

[13] 5 U.S.C. 552a(j).

appeal any denial of his request, and file a statement of disagreement if the denial and appeal result in a stand-off, either before or after judicial review. In allowing the individual to file a statement of disagreement, even after the agency's denial of his request is upheld by a court, the Act implicitly recognizes that the agency and the individual may have divergent interests in the content of a record, as well as the fact that there may be no clear-cut criteria for assessing accuracy, timeliness, completeness, or relevance.

Despite the Act's sophistication in this area, however, the correction and amendment rights have not been widely exercised. This doubtless reflects the small number of access requests under the Privacy Act; but it may also be due in part to the fact that so many of the agency records an individual might want to correct or amend are exempt from the individual access requirement and therefore not open for correction or amendment. Nevertheless, the right to correct or amend a record, once access has been obtained, is an area in which the Privacy Act represents a significant advance for the individual.

The Collection Limitation Principle

The fourth principle of the Privacy Act is that there shall be limits on the type of information a record-keeping institution collects about an individual, as well as certain requirements with respect to the manner in which it may be collected. An agency may not collect whatever information it wishes, nor may it collect information in whatever manner it wishes. The principle is implemented by requiring that agencies (1) collect only information that is relevant and necessary to accomplish a lawful purpose;[14] (2) collect information to the greatest extent practicable directly from the subject individual;[15] (3) give every individual a Privacy Act Statement at the time individually identifiable information is requested of him;[16] and, (4) in certain instances, refrain from collecting an individual's Social Security number[17] and information relating to his exercise of First Amendment rights.[18]

The requirement to limit collection to information that is relevant and necessary to accomplish a lawful purpose of the agency seems to have resulted in a modest amount of revision and reduction of data-collection forms, and consequently a modest reduction in data collection itself. In contrast, the requirement that agencies collect information to the greatest extent practicable from the subject individual does not appear to have changed practices at all.

The required "Privacy Act Statement" seems not to have had much of an effect on the amount of information individuals are asked to provide about themselves or on their willingness to provide it. There appears to have been a slight reduction in the willingness of individuals to answer survey

[14] 5 U.S.C. 552a(e)(1).
[15] 5 U.S.C. 552a(e)(2).
[16] 5 U.S.C. 552a(e)(3).
[17] Section 7 of Public Law 93-579.
[18] 5 U.S.C. 552a(e)(7).

questions since passage of the Act, but this cannot be confidently attributed to the Privacy Act Statement.

In addition, there appears to be some troublesome ambiguity in the subsection of the Act that contains the "Privacy Act Statement" requirement. Subsection 3(e)(3) reads in part:

> Each agency that maintains a system of records shall—
>
> (3) inform each individual whom it asks to supply information . . .

Some agencies have interpreted this to require a statement only when individually identifiable information is collected from the subject individual and not to require it when such information is collected from a third party. The Commission believes that *a Privacy Act Statement should be provided to all individuals from whom individually identifiable information is collected, including third parties.*

On the other hand, the Privacy Act Statement must now be supplied or read each time individually identifiable information is collected, regardless of the frequency of contact between an agency and an individual. This is burdensome to the agency and can cause the Statement to be ignored by the individual. The purpose of the Statement is to provide the individual with enough information to allow him to judge whether or not to provide the information requested. There appears to be no useful purpose in doing this repeatedly if the individual has been provided with a copy of the Statement within a reasonable period of time prior to a follow-up request for information so long as the follow-up request is consistent with the original statement. Thus, the Commission believes that *the burden on agencies could be safely reduced by requiring that the individual be given a Privacy Act Statement only if he had not already been given a retention copy within a reasonable period of time prior to a subsequent request for information from him.*

A second problem with the Privacy Act Statement is that it tends to state the obvious and does not explicitly spell out other possible uses of the information. The Commission, consistent with its recommendations in other areas, believes that *the Statement should describe those uses of information that could reasonably be expected to influence an individual's decision to provide or not to provide the information requested.* Since the individual's decision may be influenced by the techniques used to verify the information he provides, *the Statement should also include a description of the scope, techniques, and sources to be used to verify or collect additional information about him.*

Providing a concise statement on uses and third-party sources may, upon occasion, prove to be more confusing than enlightening. Therefore, the Statement should, in addition, *identify the title, business address, and business telephone number of a responsible agency official who can answer any questions the individual may have about the Privacy Act Statement.*

The proscription on the collection of information about how an individual exercises his First Amendment rights appears to have had no noticeable effect on agency collection practices. The prohibition does not

apply when an agency is expressly authorized to collect such information either by statute or by the individual, or where collection is "pertinent to and within the scope of an authorized law enforcement activity." *[5 U.S.C. 552a(e)(7)]* Because virtually all government agencies can be said to be involved in some type of law enforcement, the latter exception, in particular, has tended to negate the prohibition. A more accurate, and hence more effective, way of stating the congressional intent would be to refer to "an authorized investigation of a violation of the law." This change would not prohibit an agency from collecting a specific item of information whose collection is expressly required by statute or expressly authorized by the individual to whom it pertains, or whose collection would be a reasonable and proper library, bibliographic, abstracting, or similar reference function.

Section 7 of the Privacy Act, which attempts to limit collection of the Social Security number from individuals, also appears to have had little effect on agency practice. Its "grandfather clause," which allows agencies to continue to demand the number if they did so under statute or regulation prior to January 1, 1975, has encompassed almost all uses of the Social Security number at the Federal level, as indicated in Chapter 16 below.

The Use Limitation Principle

The fifth Privacy Act principle asserts that, once collected, there are limits to the *internal* uses to which an agency may put information about an individual. Once an agency has legitimately obtained information, it still may not use it internally without restriction.

The Act requires an agency to obtain an individual's written consent before disclosing a record about him to any of its employees other than "officers and employees . . . who have a need for the record in the performance of their duties." *[5 U.S.C. 552a(b)(1)]* However, because the terms "need" and "duties" are open to interpretation, the effect of this restriction is limited.

In theory, the requirement speaks to the kind of situation described in Chapter 6, wherein the employee-employer relationship was seen to subsume other record-keeping relationships, such as the medical-care and insurance ones. A problem inherent in the provision is the fact that one agency may have many different types of relationships with an individual but the provision takes no account of the difference between them; for that reason it has no practical effect on limiting certain internal uses of information. This is particularly true in the case of the larger cabinet departments which, for purposes of the Privacy Act, have defined themselves as one "agency."

Where differences in record-keeping relationships have been recognized in other statutes, such as where a component of the Department of Health, Education, and Welfare is subject to a confidentiality statute elsewhere in the U. S. Code, the integrity of the relationship that the statute addresses may be preserved within the framework of Subsection 3(b)(1). Section 1106 of the Social Security Act, for example, limits the disclosure of records maintained by the Social Security Administration, and thus it

functions as a limitation on internal agency uses of records, even though the Department of Health, Education, and Welfare has defined itself as one agency for the purposes of the Privacy Act.

It can reasonably be assumed that the Privacy Act was not intended to nullify other statutes which limit the use and dissemination of information. Indeed, while the Act is silent on this issue, the OMB Guidelines advise that: "Agencies shall continue to abide by other constraints on their authority to disclose information to a third party including, where appropriate, the likely effect upon the individual of making that disclosure."[19] One would expect the OMB guidance to be definitive, but the internal use issue is a murky one. The "confidentiality" statutes in the U.S. Code are many and various, and it is not clear how statutes that *authorize* use or disclosure, rather than *prohibit* it, should be treated in relation to Subsection 3(b)(1).

The Commission believes that *the way to resolve this issue is through a revised routine-use provision that would apply to both internal and external agency uses and disclosures of information.* Such a provision would act as a minimum standard against which potential uses and disclosures of information would be measured. It would supersede preexisting statutes that authorize disclosures in a vague or general manner, but not statutes in which the Congress, as a matter of public policy, has called for the use and disclosure of specific types of information in specific situations. Such a provision, moreover, would not be construed as expanding an agency's authority to use or disclose information if the agency was already subject to a preexisting statute that restricted its use and disclosure of information more narrowly than the Privacy Act does.

The only way for the individual to discover the internal agency uses of a record about himself is through the "Privacy Act Statement," which cannot anticipate future uses over which the agency has no control. For example, two days after the Privacy Act was passed, the Congress passed another law creating a Federal Parent Locator Service (PLS) authorized to obtain information from the Social Security Administration upon request, regardless of the strictures of other statutes such as the Privacy Act. As already noted, moreover, the "Privacy Act Statement" need not inform the individual that information about him may be collected from third parties, thereby diluting the effect of the Use Limitation Principle even further.

While the Commission believes that the problem of controlling internal uses of information cannot be solved by levying specific requirements on the agencies, *the "routine use" provision, which forbids disclosures that are not compatible with the purpose for which the information was originally collected, should be applied to internal agency uses.* In addition, by strengthening the individual enforcement mechanism and establishing a central office within each agency for Privacy Act implementation (see below), compliance with the spirit of the internal use requirements will be improved.

---

[19] Office of Management and Budget, Circular A-108, *op. cit.*, p. 28953.

The Disclosure Limitation Principle

The sixth Privacy Act principle asserts that there must be limits on the *external* disclosures of information an agency may make. That is, once an agency has legitimately obtained information, it still may not disclose it externally without restriction.

The Privacy Act authorizes ten categories of external disclosures that may be made without the consent of the individual. The most important one is found in Subsection 3(b)(3) which authorizes any disclosure that has been established as a "routine use"; that is, any disclosure for a "purpose which is compatible with the purpose for which [the information] was collected." *[5 U.S.C. 552a(b)(3); 5 U.S.C. 552a(a)(7)]* The key word is "compatible," which some agencies have interpreted quite broadly. As but one example, the United States Marshals Service published a routine-use notice on September 16, 1976, which read in part:

> A record may be disseminated to a Federal agency, in response to its request, in connection with . . . the issuance of a license, grant, or other benefit by the requesting agency, *to the extent that the information relates to the requesting agency's decision on the matter.*[20] [emphasis added]

Other agencies, however, have interpreted the routine-use provision narrowly. Prior to passage of the Privacy Act, the Railroad Retirement Board (RRB) obtained benefit and employee name and address information from the Social Security Administration (SSA) to check the accuracy of payments made to claimants under the Railroad Unemployment Insurance Act (RUIA). The statute requires RUIA benefits to be calculated in the light of all other social insurance, employment, or sickness benefits payable to an individual by law. Today, however, the RRB is no longer obtaining information from the SSA, because the SSA has concluded that it cannot legitimately establish the disclosure as a routine use. The RRB estimates that this is costing it more than $85,000 a year in unnecessary payments.

Another problem with the routine-use provision for disclosures in Subsection 3(b)(3) is its relation to Subsection 3(b)(7), which authorizes disclosures of individually identifiable information to agencies for law enforcement purposes if the head of the agency requests the information in writing and specifies the legitimate law enforcement activity for which the information is desired. While treating the routine-use provision narrowly for some purposes, most agencies have employed it in combination with other laws to facilitate the flow of information to and between law enforcement and investigative units.

The combination of the Privacy Act's routine-use provision and Section 534 of Title 28, for example, permits agencies to circumvent the requirements of Subsection 3(b)(7). Under Section 534 of Title 28, the Department of Justice is required to maintain a central law enforcement information bank and to provide a clearinghouse for such information, particularly for agencies of the Federal government. Agencies have

[20] *Federal Register*, Volume 41, Number 181, September 16, 1976, p. 40015.

understood this provision to be a congressional endorsement of the routine exchange of law enforcement information, at least under the auspices of the Attorney General.

Currently, agencies of the Federal government seem to be employing the routine-use provision in order to permit the free flow of law enforcement and investigative information without having to comply with the standards of Subsection 3(b)(7). Agency system notices frequently indicate that information will be supplied to appropriate Federal, State, local, and, sometimes, foreign law enforcement agencies of government. In short, the Privacy Act does not place an effective burden on, or barriers to, the free flow of information within the law enforcement and investigative community.

Concurrent with formal endorsement of relatively unrestricted information flow to and between investigative agencies, the agents of investigative units have continued to employ the informal information network that exists within the law enforcement community. An agent of one unit may call his counterpart in a second agency to see if it might have any information on the subject of an investigation or any leads to people who might be appropriate to investigate. As the system currently operates, there would be some impediments to such disclosure—though not insurmountable ones—where the units of government involved only investigative agencies and the information exchanged came exclusively from their files. Today, however, the unfettered ability to exchange information between law enforcement and investigative units amounts to access by such units to virtually any governmental records without the need to comply with the strictures in Subsection 3(b)(7).

Almost all agencies have law enforcement units of one sort or another through which information desired by other units in other agencies may be channeled. Indeed, the law enforcement unit of an agency might seek information on an individual from records maintained by other components of an agency and transmit it to a second agency which could subsequently maintain it in a form (e.g., retrievable by docket number) which leaves it free of Privacy Act restrictions. Law enforcement units and investigation agencies can, and often do, operate in this fashion and thus function as a conduit for the exchange of information with other law enforcement units. The problem is not so much that law enforcement units disclose information about individuals to illegitimate recipients, but rather that the determination of legitimacy is more often than not highly informal, with the decision to disclose being made by anyone from the field agent level to the head of an agency. Such informality presents substantial potential for improper disclosure. This is a problem the Commission has not dealt with extensively, though a structure for effective examination of it is suggested later in this chapter.

Although the effect of the routine-use provision has been limited, due mainly to the fact that it has been interpreted as applying only to external transfers of information, its safety-valve aspects should be preserved. The disclosure provisions of the Privacy Act must allow for a certain amount of agency discretion, since, in an omnibus statute, it is impossible to enumerate

all of the necessary conditions of disclosure. Nonetheless, the Commission believes that *the compatible-purpose test of the routine-use provision should be augmented by a test for consistency, with the conditions or reasonable expectations of use and disclosure under which the information was provided, collected, or obtained.* The individual's point of view must be represented in the agency's decision to use or disclose information, and today the compatible-purpose test only takes account of the agency's point of view.

The routine-use definition should also apply to internal, as well as external, agency uses and disclosures of information. This is important, since the majority of uses of information are made by the agency that originally collects it.

Congress may, of course, elect, as it has done in the Tax Reform Act of 1976, to authorize particular uses or disclosures of information that are either incompatible with the purpose for which the information was collected, or inconsistent with the individual's reasonable expectations of use and disclosure. Such additional uses and disclosures of information should be treated as routine uses, provided that the statute authorizing them establishes specific criteria for use or disclosure of specific types of information. Ideally, the Congress should review all the statutes that authorize such incompatible uses and disclosures and determine which ones it wishes to retain. The point, however, is that the Commission, as in other areas, believes that blanket disclosure authorizations or limitations should be actively discouraged.

One might think of incompatible uses and disclosures as "collateral uses." The question of whether a particular use or disclosure qualifies as a "collateral use" would then arise only after it has been established that the proposed use or disclosure was not a "routine use." The "collateral use" concept would also give the Congress a means of relating subsequently enacted disclosure statutes to the Privacy Act so that there will be no question about whether such disclosures are subject to the Act's requirements. As indicated earlier, and as discussed more thoroughly in Chapter 14, the Tax Reform Act of 1976 is a good example of how this would work.

Besides resolving the routine-use issue, there is also a need to take explicit account in the Act of agency disclosures concerning constituents of Members of Congress. In the early days of the Act's implementation, Congress had trouble obtaining information for its own use. Congressional caseworkers found that they were unable to get individually identifiable information from agencies when they called them on behalf of constituents. Agencies refused to give out information to Members of Congress unless they received prior consent from the individual, since Subsection 3(b)(9) only authorizes disclosures to congressional committees or to the House or Senate as a whole. Members of Congress felt this undermined their role as representatives of their constituents, and it was, in fact, an oversight in the drafting of the current law.

To solve this problem, the Office of Management and Budget

suggested to agencies that they establish disclosures to congressional offices as a routine use,[21] and this is now a government-wide practice. The Commission believes this practice should be allowed to continue but that a specific provision should be included in the Act to permit it, since the current solution puts a strain on the interpretation of the compatible-purpose test. Disclosure of a record should be allowed to a Member of Congress, but only in response to an inquiry from the Member made at the request of the individual involved, *provided the individual is a constituent of the Member*. Such a request could also be made by a relative or legal representative of the individual, if the individual is incapacitated or otherwise clearly unable to request the Member's assistance himself, *and the requestor or the individual is a constituent of the Member*.

Finally, some observers are of the view that, because the Privacy Act *limits* disclosures to the public, and the Freedom of Information Act *directs* disclosure to the public, there is an unresolvable conflict between the two laws. This view, however, is overly simplistic and, in the final analysis, an erroneous formulation of the relationship between the two statutes. The Privacy Act and the Freedom of Information Act mesh well. There are no statutory conflicts. Recent court decisions have also better defined the balances that must be struck between the competing interests. Nonetheless, there do appear to be some practical problems in the implementation of these two laws.

The "conditions of disclosure" section of the Privacy Act that establishes the ten categories of permissible external disclosures allows an agency to disclose a record about an individual to a member of the public who requests it, if the disclosure would be *required* under the Freedom of Information Act.[22] On the other hand, Subsection (b)(6) of the Freedom of Information Act allows an agency to refuse to disclose a record to a member of the public (i.e., anyone other than the individual to whom the record pertains) if it is a medical, personnel, or similar record, the disclosure of which would constitute a "clearly unwarranted invasion of personal privacy."[23]

To understand the meshing of these requirements, it is useful to consider first the situation prior to the passage of the Privacy Act. The exemptions on access to information in the Freedom of Information Act are discretionary, not mandatory. Thus, under the FOIA (prior to the passage of the Privacy Act), an agency *could* withhold information, the disclosure of which would, in the agency's opinion, constitute a "clearly unwarranted invasion of personal privacy," but the agency was not *required* to do so. Today, after passage of the Privacy Act, an agency is still *required*, by the Freedom of Information Act, to disclose information that would *not* constitute a "clearly unwarranted invasion of personal privacy," but now an agency no longer has the *discretion* to disclose information it believes would constitute such a clearly unwarranted invasion.

---

[21] Office of Management and Budget, *Implementation of the Privacy Act of 1974, Supplementary Guidance, Federal Register*, Volume 40, Number 234, December 4, 1975, pp. 56741-56743.

[22] 5 U.S.C. 552a(b)(2).

[23] 5 U.S.C. 552(b)(6).

A major problem in this area, however, is that agency operating personnel responsible for the day-to-day implementation of the two Acts have not been clearly enough apprised of how the laws mesh, of the applicable interpretations and court decisions, and of an agency's corresponding responsibilities under them. As a result, confusion, widely differing implementation, and occasional frustration of the intent of both laws have resulted. While determining what constitutes a "clearly unwarranted invasion of personal privacy" will always require a certain amount of interpretation, more can and should be done to assist and guide those who have to make such determinations in the course of their daily work. Indeed, one of the primary functions of the entity recommended by the Commission in Chapter 1 would be to assist agencies in developing policy to assist agency employees in making such determinations.

The Information Management Principle

The Privacy Act incorporates the principle that there are proper approaches to the management of information and that agencies should take affirmative steps to assure that their information management practices conform to a reasonable set of norms. Subsection 3(e)(1) of the Privacy Act requires an agency to:

> maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President; *[5 U.S.C. 552a(e)(1)]*

In addition, Subsection 3(e)(5) requires that:

> all records which are used by [an] agency in making any determination about an individual [must be maintained] with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; *[5 U.S.C. 552a(e)(5)]*

Further, Subsection 3(e)(10) requires an agency to:

> establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarassment, inconvenience or unfairness to any individual on whom information is maintained; *[5 U.S.C. 552a(e)(10)]*

In theory, these requirements, in combination with the requirements implementing the Individual Participation and Accountability Principles, keep the individual from having to bear the full burden of monitoring the content of records an agency maintains about him, and they also grant him recourse when he can prove damages as a consequence of willful behavior in violation of the Act's requirements.

The Act's several information management provisions have had a

positive effect on agency conduct by focusing an agency's attention on its policies and practices relating to the collection, maintenance, use, and dissemination of records about individuals. In addition, the Act's requirement that information must be relevant and necessary to accomplish a mandatory agency purpose seems to have reduced slightly the amount of information agencies maintain.[24] Likewise, the "Privacy Act Statement" requirement[25] and the annual notice requirement[26] have somewhat limited the number of systems of records. But the requirement that information be kept accurate, timely, complete, and relevant[27] appears to have had little effect on reducing or altering the types of information maintained.

Most agencies, to the extent they have a position, stand by their prior record maintenance practices. They contend that they have always attempted to achieve accuracy, and that the terms "timely, complete, and relevant" are meaningful only in the context of a specific record or record-keeping situation—which is true. Nonetheless, interviews with operating personnel suggest that, although some accuracy standards have been tightened and retention periods for documents have been re-examined, agencies continue to maintain a substantial amount of information that is not as accurate, timely, complete, and relevant as it should be. The fact is that there are few if any formal mechanisms to review existing records and there is seldom, if ever, enough time to do so.

Because no specific, consistently applied criteria have been established for determining when an agency is in compliance with the Act's information management principles, they are not being adequately implemented. Within agencies, there has often been little or no compliance monitoring, as well as no office to which agency operating personnel can turn for guidance. Although efforts to train agency personnel are being made, awareness of the Act's requirements is much weaker than it should be—in all areas, not just information management.

Generally speaking, each agency or major agency component has a nucleus of employees who are well versed in matters relating to the Privacy Act, but many middle-level and lower-level operating personnel still do not know enough about the Act to allow them to carry out their responsibilities under it. For example, the Privacy Act is too often cited as the reason for withholding information from the public, when, in fact, such withholding is improper. Yet, without training, it appears that the one thing an agency employee is likely to know about the Act is that it contains criminal penalties for unauthorized disclosures, and thus that he should behave warily, particularly in responding to third-party Freedom of Information Act requests of the sort discussed in the preceding section on the Disclosure Limitation Principle.

The Commission has found that those agencies that have established formal, structured approaches and mechanisms to implement the Privacy Act are the most successful in their implementation of the Act. They have

[24] 5 U.S.C. 552a(e)(1).
[25] 5 U.S.C. 552a(e)(3).
[26] 5 U.S.C. 552a(e)(4).
[27] 5 U.S.C. 552a(e)(5).

provided the best training for their personnel, have issued detailed, consistent internal guidelines, and have devised procedures for auditing their own compliance with the Act. In addition, agencies with previous experience with issues relating to information policy have generally adapted more readily to the requirements of the Act than have agencies for which information policy issues can be considered a relatively new experience.

In order to provide for more effective implementation of the Act, the Commission believes that *the head of each agency should designate one official with authority to oversee implementation of the Act.* The official's responsibilities would include issuing instructions, guidelines, and standards, and making such determinations, as are necessary for the implementation of the Act. He would also be responsible for taking reasonable affirmative steps to assure that all agency employees and officials responsible for the collection, maintenance, use and dissemination of individually identifiable records are aware of the requirements of the Act.

The Commission believes that this is the minimum step necessary to ensure effective implementation of the Privacy Act. It parallels, and enhances, the approach taken by the agencies which are currently most successful in their implementation of the Act. Someone other than the individual record subject must be in a position to hold agency record keepers accountable; the Act's individual enforcement model is simply ineffective on a broad scale. Moreover, someone must have the authority to make decisions under the Act (e.g., to interpret the "reasonableness" and "compatible-purpose" tests); someone must be in a position, for example, to review a particular record-keeping practice or computer system design and assert, with authority, that it is reasonable. Obviously, such an approach addresses more than information management, and it can reasonably be expected that the designated agency official's activities would span the gamut of issues relating to the Act's implementation.

The Commission looks with favor on the Act's basic assumption that each agency is in the best position to judge what is best, reasonable, or appropriate for it. As indicated in the implementation in Chapter 1, it favors abandonment of the individual agency autonomy model of the Privacy Act only in instances where a clear societal interest is at stake or where it is necessary to establish an independent check on the agency.

Strengthening the individual agency enforcement mechanisms in the Privacy Act by the appointment of a Privacy Act officer in each agency is not intended to relieve the agency's operating personnel of their responsibilities under the Act. Rather, it is intended to make their jobs easier by providing a mechanism for guidance, instruction, and interpretation. A "reasonableness" test in the law is important for a court, but it does little to provide insight and guidance for those charged with the day-to-day implementation of the law.

By the same token, creation within an agency of an enforcement mechanism will serve to hold agency employees accountable in a way that no external entity or individual record subject can. This is as it should be, for ultimately the record-keeping agency must bear the burden for assuring that its record-keeping practices are fair.

While the Commission found that the Act's requirements regarding the necessity, accuracy, timeliness, completeness, and relevance of information in records *[5 U.S.C. 552a(e)(1); 5 U.S.C. 552a(e)(5)]* appear to have had little effect on agency practices, it suggests no specific changes in those requirements. Rather, it believes that by altering the implementation strategy and incentives for compliance along the lines it suggests, the goals of these requirements will be achieved.

The Commission has also found that the Act's requirements for propagation of corrections does not adequately assure that decisions are made on the basis of accurate, timely, complete and relevant information. Under the Act, for example, corrections do not have to be sent to prior internal agency recipients or to the sources of erroneous information. In addition, corrections of erroneous information initiated by the agency rather than by the individual, no matter how important, do not have to be propagated at all. As in other areas it has examined, the Commission believes that *corrections made by the record-keeping agency, as well as those made by the individual, should be propagated; and that, with some exceptions, corrections should be sent automatically to sources and prior internal and external recipients who provided or received the erroneous information, within a reasonable period of time prior to the making of the correction, as well as to any person (organization or individual) the individual specifically designates.*

The Commission believes that corrections of erroneous information by the agency, in accordance with the Act's requirements to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, timeliness, completeness, and relevance as is reasonably necessary to assure fairness . . ." *[5 U.S.C. 552a(e)(5)]* should be automatically propagated if two conditions exist: first, if the correction could reasonably be expected to affect a determination about the individual by the source or a prior recipient of the erroneous information that provided or received the information, within a reasonable period of time prior to the making of the correction; and second, if the source or prior recipient could not reasonably be expected to otherwise become aware of the error. However, propagation should not be required to prior recipients who received the erroneous information under the Freedom of Information Act or to any source who, acting on his own behalf, rather than in an official capacity, provided the erroneous information to the agency.

This approach provides for propagation of corrections in cases in which they would make an important difference to the individual, while limiting to the greatest extent possible the burden on the agency. Relating the propagation requirement to the Act's fairness-in-decision-making provision is important because doing so excludes certain corrections, such as those made to keep an historical record accurate.

The Commission believes it appropriate to place the basic responsibility for propagating corrections on the agency because there is no other realistic way for the individual to protect himself against the spread of erroneous information about him through the Federal government. Information can flow so freely within and between agencies, and decision points are so diffuse or difficult to isolate, that linking a propagation of correction

requirement to an adverse determination, or to an initiative by the individual, destroys its efficacy.

By including the requirement that corrected information be sent to internal agency recipients and to sources, the Commission is also responding to evidence that suggests that more harm or unfairness can result to an individual from inaccurate internal agency uses and disclosure than from external uses and disclosures, since the former are more frequent and less apt to be independently verified. The requirement that an agency notify any person specifically named by the individual to whom the information pertains, of any corrections made by either the individual or the agency, is included to allow for propagations that the individual determines are important to him.

The Privacy Act requirement to maintain an accounting of disclosures of information about an individual is widely regarded as the statute's single most burdensome provision. It also appears to be one which has engendered little interest on the part of the general public. There are three objectives which can be potentially served by this requirement: (1) providing the record subject with a listing of the uses and disclosures of a record about him; (2) facilitating the propagation of corrections; and (3) internal agency auditing and compliance monitoring. Currently, the emphasis is on the first objective. Consequently, the Act, with two exceptions, requires an accounting of disclosures to every recipient of information from a system of records, including the individual himself, and the accounting must include the date, nature, and purpose of the disclosure, as well as information identifying the recipient. This required accounting is frequently burdensome, as well as occasionally unnecessary, and has led a number of Federal agencies to construe it as inapplicable in cases in which the individual is the recipient of the information. Moreover, an accounting does not have to be kept of internal agency uses and disclosures, and these are frequently of the most interest to the individual and the most important insofar as the propagation of corrections is concerned.

The Commission believes that *the primary emphasis of the accounting of disclosure requirement should be on its utility in propagating corrections and that a "reasonableness" test should be established for determining the period of time for which an accounting must be kept, as well as for the amount of detail about each disclosure that must be kept.* In addition, the Commission believes that *when an individual so requests, an agency should make available to him its accounting of disclosures about him to (a) all prior recipients to whom it could reasonably be expected to propagate corrections, and (b) other recipients of which it could reasonably be expected to be aware.* This would allow an individual to see the information an agency must maintain on its disclosures about him for the purpose of propagating corrections automatically, but would not require a log in any greater detail than that. This requirement, coupled with the suggested propagation of corrections requirement, would, however, mean that an individual would be able to obtain an accounting of disclosures to *internal agency recipients* of information, as well as to external ones, since under the new approach all prior internal recipients will now receive corrections when they are propagated.

An agency should be left free to decide how long to keep an accounting of disclosures based on its determination of how long it needs to keep the information for propagating corrections, as well as the amount of detail that needs to be kept about each disclosure. In all accountings disclosed to the individual, however, an agency should take reasonable affirmative steps to inform the individual, in a form comprehensible to him, of the date, nature, and purpose of each disclosure and the name and address of the person or agency to whom the disclosure was made.

One principal difference between this approach and the Act's accounting requirement is that an accounting would not need to be kept for five years, or the life of the record, whichever is longer.[28] The Commission would also preserve the Act's use of the word "accounting" as opposed to "record," in order to allow for any scheme that enables the agency to reconstruct a list of past disclosures; that is, an explicit record or log entry need not be made for each disclosure. This is especially important in the case of frequent bulk transfers of data (when even the nature and purpose may only be generally known.)

The Privacy Act requirement that agencies establish safeguards to assure the security of individually identifiable records[29] has run the gamut from business-as-usual to extreme measures aimed at forestalling any conceivable risk, no matter how small its chance of occurring. On balance, however, the "safeguarding of information" requirement has resulted in minor modifications, and some strengthening, of agency data-security standards.

A recently publicized example of a government information system with inadequate security involved the computer and telecommunications system, SSADARS, which connects private insurance companies acting as Medicare intermediaries for the government with the Social Security Administration (SSA) data file. The Social Security Administration reported at the Commission hearings on Medical Records in July 1976 that its longstanding policy of protecting the confidentiality of individually identifiable information in its files had been adequately carried out in its administrative and technical safeguards. On October 23, 1976, however, SSA announced that it had discovered that it was mistaken in its belief that there was "no way the Medicare intermediaries and carriers can use their telecommunications system to gain access to the files used to administer"[30] other SSA programs. SSA staff found that the SSADARS terminals installed in the offices of two intermediaries could have been altered relatively easily, thereby permitting access to files other than the Medicare eligibility files the intermediaries needed to see. Although no actual access to other SSA program information is believed to have occurred, the technical safeguards to assure the confidentiality of information in the SSADARS system were not as effective as SSA had thought.

---

[28] 5 U.S.C. 552a(c)(2).

[29] 5 U.S.C. 552a(e)(10).

[30] Written statement of the Bureau of Health Insurance, Social Security Administration, *Medical Records,* Hearings before the Privacy Protection Study Commission, July 20, 1976, p. 11.

In spite of the Privacy Act, and assurance by the Social Security Administration that insurance company employees are subject to criminal sanctions as if they were Federal employees, SSA's Data Acquisition and Response System (SSADARS) has created a great deal of concern among the public and press. Inasmuch as the SSADARS system is a forerunner of the type of computer and telecommunications system which would be necessary for the administration of a broad-based Federal health-insurance program, it is imperative that Federal agencies take immediate affirmative measures to prevent information in such a system from becoming a source of unfairness to the individuals to whom it pertains. Therefore, the Commission recommends:

Recommendation (1):

That a Federal agency administering a health-insurance program which employs the services of a private health-insurance intermediary provide to the intermediary only that information necessary for the intermediary to carry out its responsibilities under the program.

Compliance with this recommendation would require that Federal agencies administering health-insurance plans develop administrative, physical, and technical safeguards as required by Section 3(e)(10) of the Privacy Act to assure the integrity of, and to prevent unauthorized access to, federally maintained data bases.

To correct the drafting deficiencies in the current safeguard requirement, as well as to make the obligation imposed by the requirement more realistic, the Commission believes that *an agency should be required to establish* reasonable *administrative, technical, and physical safeguards to assure the integrity, confidentiality, and security of its individually identifiable records so as to minimize the risk of substantial harm, embarrassment, inconvenience, or unfairness to the individual to whom the information pertains.* Such a change would be consistent with the Act's legislative history and should protect against the overreaction occasioned in some agencies by the current language of the Act which requires agencies to establish *appropriate* safeguards against *any anticipated threats or hazards.*

There is another related issue which also must be addressed. The Commission was specifically required by Subsection 5(c)(2)(B)(iv) of Public Law 93-579, to examine the issue of:

> whether and how the standards for security and confidentiality of records under section 3(e)(10) of [the Privacy Act] should be applied when a record is disclosed to a person other than an agency.

The use of the word "standards" in this directive raises the question of the type of standards contemplated by the drafters. Within the Federal sector, the term standards has a precise meaning, and there are well defined procedures for establishing Federal Information Processing Standards (FIPS). A standard may be considered as synonymous with a "requirement," and, once established, is binding on Federal agencies. On the other hand, the term "guideline" may be equated with a "suggestion," and is not

binding on Federal agencies. It seems clear from a reading of the Act and the legislative history, however, that the drafters did not intend the term standards, as used in Subsection 5(c)(2)(B)(iv), to be interpreted precisely, but rather to be interpreted more broadly as meaning "general criteria" for the establishment of security and confidentiality safeguards. Regardless of the meaning intended, however, the conclusion of the Commission remains the same.

The Commission's inquiry has shown that there are currently no standards, in the strict sense of the word, for security and confidentiality at the Federal level. Guidelines have been issued by the National Bureau of Standards, but their specificity and hence their utility is uneven. FIPS Publication No. 31,[31] which establishes guidelines for automatic data processing physical security and risk management, is much more detailed and specific than FIPS Publication No. 41,[32] which is intended to establish computer security guidelines for implementing the Privacy Act of 1974. As already noted, the Commission's assessment of the Federal experience indicates that agency practice in response to the safeguard requirement in Subsection 3(e)(10) is extremely varied, ranging from no response whatsoever to what could be termed technological overkill. At the Federal level, in other words, there are, at best, limited standards, guidelines, or general criteria for safeguards which are susceptible to extension to any non-Federal agency recipient of information subject to the Privacy Act. Thus, in response to the mandate given it in Subsection 5(c)(2)(B)(iv), the Commission recommends:

Recommendation (2):

That there should be a continued examination of the standards, guidelines, and general criteria for safeguards within the Federal government, but there should not be a general extension of any Federal standards, guidelines, or general criteria for safeguards for security and confidentiality of records when a record is disclosed to a person other than an agency, except as specifically provided in other recommendations of the Commission.

The Accountability Principle

The eighth principle of the Privacy Act holds that an institution should be accountable for its personal-data record-keeping policies and practices, or, more specifically, for adherence to the other seven information policy principles. Under the Privacy Act, a Federal agency can be held accountable for its record-keeping policies and practices in several ways. The individual can hold the agency accountable through exercise of his rights to see, copy, and challenge the contents of a record about himself, to review an

[31] National Bureau of Standards, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, June, 1974.

[32] National Bureau of Standards, *Computer Security Guidelines for Implementing the Privacy Act*, May 30, 1975.

agency's accounting of disclosures made of a record about him, and to sue for any damages he incurs as a consequence of agency misconduct. In addition, agency employees are subject to criminal sanctions for particular violations of the law's requirements.[33]

The access, correction, and amendment procedures have been discussed. They appear to work reasonably well, although they have not been widely used. As previously noted, the agencies regard the Act's accounting of disclosures requirement as the most burdensome of the Act's provisions. It represents 26 percent of the operating costs of the Act[34] and requires extra effort by agency employees on an almost daily basis. The Social Security Administration, which keeps its accounting of disclosures manually, has stated that to perform the accounting effectively it would have to totally redesign its computer system. In addition, few individuals have asked for an accounting of the disclosures made of a record about them, perhaps because they do not know they have a right to do so. Even when an individual does ask, however, he will not learn about internal agency disclosures, as no accounting need be kept of them.

The civil remedies provided by the Act are similarly ineffective from the individual's point of view. The vast number of systems involved,[35] the need to establish willful or intentional behavior on the part of the agency, and the cost and time involved in bringing a law suit, often make enforcement by the individual impractical. Moreover, an individual must show actual injury in all cases except the ones that can be brought to force an agency to allow an individual to see and copy, or correct or amend, a record.

The criminal penalties also require a showing of willfulness and apply only to unauthorized disclosures, failures to publish annual system notices, and obtaining a record from an agency under false pretenses. The circumstances in which an individual can bring suit, his possible reward for doing so, and the instances in which a court can order an agency into compliance with the Act are all too limited to provide an effective accountability mechanism. Consistent with its recommendations in other areas, the Commission believes that *a suit should be permitted to force compliance with the requirements of the Act absent a demonstration of injury to, or adverse effect on, the individual and that a court should be able to order an agency to comply.*

In many cases, it is simply too difficult to show injury or adverse effect as a result of a violation of the Privacy Act. In the case of a violation of the notice requirements, for example, such a showing is most likely impossible. Even in the case of inaccurate information, it can be difficult to demonstrate actual injury. Hence, the Commission believes an individual should be granted standing without the requirement to show injury. While it could be argued that this will encourage frivolous law suits, experience to date indicates that it is not likely to do so. Moreover, this approach should

[33] 5 U.S.C. 552a(i).

[34] Letter from Hon. Bert Lance to Senator Ribicoff, *op. cit.*

[35] As of December 21, 1975, there were 6,723 systems of records of varying size containing 3.8 billion records about individuals which had been declared.

increase agency accountability and provide agencies with increased incentives to comply with the Act in order to avoid law suits by individuals.

Under the Privacy Act contractors and grantees are not directly liable for violations (although they are subject to the Act's criminal penalties) and the government may indemnify them for any civil liability resulting from their performance of a contract. This defeats the intent of the Act. If the Act's protections are so important that the government is waiving its sovereign immunity and thus subjecting itself to civil liability, it would seem reasonable for the same standard to apply to contractors and discretionary grantees, as discussed earlier. Therefore, the Commission believes that *contractors and grantees which fall within the scope of the Act should be made civilly liable under the Act in the same manner that the government makes itself civilly liable; and no official or employee of any Federal agency should include or authorize to be included in any contract or grant any provisions indemnifying the contractor or grantee from civil liabilities under the Act.*

In a related area, the Commission's mandate specifically required an examination of "whether the Federal government should be liable for general damages incurred by an individual" when an agency violates his rights under the Act. *[Section 5(c)(2)(B)(iii) of Public Law 93-579]* This required consideration of whether the current liability standard in the statute which limits recovery to "actual damages" should be broadened. To reach a judgment on the appropriate recovery standard, the Commission needed to answer two questions: (1) what the definitions of actual and general damages are or ought to be; and, (2) what the costs and benefits of each would be were it to be the Act's standard for recovery against the government.

Traditionally, damages have been divided into two classifications, general and special. Compensation for *any* injury done to an individual is available under a claim of general damages. An individual can make claims for losses due to pain and suffering, for example, even though it is impossible to fix a precise dollar value to such an injury. Special damages, on the other hand, only compensate for injury that has caused clear economic loss to the individual. The Commission has found that there is no generally accepted definition of "actual damages" in American law, but the Commission has concluded that, within the context of the Act, the term was intended as a synonym for special damages as that term is used in defamation cases. For that reason, the Commission believes the phrase "actual damages" should be discarded in favor of the more traditional and clearer term, special damages.

In addition, special damages in defamation cases are more limited than in other situations; the injuries clearly covered by them are loss of *specific* business, employment, or promotion opportunities, or other tangible pecuniary benefits. Injuries not provided for are those which may be labeled intangible: namely, loss of reputation, chilling of constitutional rights, or mental suffering (where unaccompanied by other secondary consequences).

The legislative history and language of the Act suggest that Congress meant to restrict recovery to specific pecuniary losses until the Commission could weigh the propriety of extending the standard of recovery. It has

determined that the arguments in favor of extending recovery to general damages, within dollar limits, appear stronger than the arguments against such extension.

The restriction on recovery articulated in the "actual damage" standard of the Privacy Act reflects the ancient limitation on governmental liability embodied in the principle of sovereign immunity. Arguments in support of this limitation of liability focus primarily on the need to protect the public purse and the problems involved in making the government fully responsible for the vast scope of its operations, which it has no practical means of controlling. One set of counter-arguments to this position derives from notions of fairness, which require both that wrongdoers be responsible for their wrongdoing and that those who benefit from governmental activity be asked to pay the price of their enjoyment, instead of letting that cost fall wholly on the small group of injured parties. Another counter-argument derives from basic notions of social utility. If the costs of government information practices are borne by the government, it is in a better position to decide whether the benefits of the activity outweigh their costs. In other words, restricting liability only restricts the incentive for government to reform its practices.

If the rights and interests established by the Privacy Act are worthy of protection, then recovery for intangible injuries such as pain and suffering, loss of reputation, or the chilling effect on constitutional rights, is a part of that protection. There is evidence for this proposition both in the cases which have already been brought under the Act and in common law privacy cases. Thus, to protect individuals under the Privacy Act more fairly and effectively, while ensuring that recovery does not become too burdensome, and to clarify the meaning of the Act, the Commission recommends:

Recommendation (3):

That the Privacy Act of 1974 permit the recovery of special and general damages sustained by an individual as a result of a violation of the Act, but in no case should a person entitled to recovery receive less than the sum of $1,000 or more than the sum of $10,000 for general damages in excess of the dollar amount of any special damages.

In addition to the individual's enforcement opportunities and the modest oversight role assigned to the Office of Management and Budget (OMB) *[Section 6 of Public Law 93-579]*, the Act also requires that reports on new or materially altered record systems be sent to OMB and both Houses of Congress *[5 U.S.C. 552a(o)]*, and to the Privacy Protection Study Commission. *[Section 5(e)(2)(A) of Public Law 93-579]* None of these bodies, however, has had the staff nor the consolidated expertise necessary to evaluate each report submitted. Furthermore, there is no agreement on how to assess the potential impact of a proposed system change along the lines called for in the Act, that is:

> the probable or potential effect . . . on the privacy and other

> personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers. *[5 U.S.C. 552a(o)]*

Currently, although this requirement has had the healthy effect of forcing agencies to examine the need for, and the details of, the particular system, the kind of information needed to evaluate it is not always supplied nor is it always presented in enough detail to permit an in-depth and independent evaluation of the system in question.

Given this weak enforcement framework and the flexibility of interpretation many provisions of the Act allow, there are few incentives for more than minimal compliance with most of its provisions. For example, there is a universal lack of post-award monitoring of contractor performance; and as previously noted, many agencies have not established any effective internal compliance monitoring procedure. This can be partly explained by the fact that Congress appropriated no additional funds for Privacy Act implementation. While many of the requirements of the Act represent procedures or steps that the agencies should have been following anyway, there is still cost associated with them.[36] In addition, attention to information policy issues is not usually a priority concern of agency personnel. While many employees view the Privacy Act and the issues it raises as important, a sizeable number still see the Act as a nuisance and an impediment to the performance of their agency's missions and functions.

OTHER POLICY ISSUES TO BE ADDRESSED

There are some important information policy issues the Act either ignores or does not address adequately. For example, in almost any discussion of the intent of the Privacy Act, mention is made of limiting the amount of information agencies actually collect about individuals. There is a commonly held belief, evident in the Act's legislative history and voiced by numerous agency personnel, that the Act was intended to reduce the amount of information the Federal government collects about individuals. Yet the fact of the matter is that the Act only establishes the outer boundaries of legitimate government inquiry, and it does so in a way that reflects rather closely the boundaries that had grown up prior to the Act's passage. Similarly, as the discussion of the routine-use provision indicated, transfers of information among agencies have only been slightly reduced as a result of the Act's passage.

While the Section 7 proscription against compelling an individual to divulge his Social Security number, unless specifically required by law to do so, has induced minimal change in agency practice, agencies commonly rely on Executive Order 9397,[37] issued in 1943, when they can find no other authority for demanding the Social Security number. Additionally, once the

[36] Letter from Hon. Bert Lance to Senator Ribicoff, *op. cit.*

[37] *Federal Register*, Volume 8, Number 237, November 30, 1943. This order provides that whenever a head of a Federal agency "finds it advisable to establish a new system of permanent

Social Security number is collected, its use is regulated only by the other disclosure provisions of the Privacy Act or whatever other confidentiality statutes govern agency disclosures of other types of personal information.

The Privacy Act grew out of nearly a decade of congressional examination of information systems in the Executive branch, and it followed closely on the heels of the record-keeping abuses and invasions of personal privacy associated with the Watergate affair. It was passed partially as a protection against premeditated abuses of Federal agency records but, more importantly, in recognition of the fact that even normal uses of a record about an individual can have harmful consequences for him and that this potential harm can be greatly magnified by the use of emerging computer and telecommunications technology. Despite these antecedents, however, there is little in the Privacy Act to prevent premeditated abuses of power through the misuse of recorded information, particularly where internal agency uses are concerned. Although the individual's position in relation to an agency is much stronger as a result of the Act, the safeguard provisions have not been implemented in a way that adequately deters abuse by agency personnel, especially in view of the lack of internal agency compliance monitoring or auditing.

Moreover, the problems perceived by the Congress at the time of the Act's passage have turned out to be more complex than anticipated, and by and large they are independent of the problem of premeditated abuse. Actual or potential information abuses are much more likely to result from continuing growth in the government's appetite for information about individuals and in the use of that information for growing numbers and types of purposes. *The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.* Dramatic developments in computer and communications technology, which both facilitate record-keeping functions previously performed manually and provide the impetus and means to devise new ones, can only exacerbate this problem.

The Act's failure to attend to the impact of technological advances on individual liberties and personal privacy is compounded by the manual, or file-cabinet, view of record keeping that underlies it. As indicated early in this chapter, reliance on a traditional view of individual identifiers and their role in retrieving records serves to exclude certain types or forms of individually identifiable records from the Act's coverage. Because a record retrieved by attribute or characteristic, as opposed to identifier, does not fall within the definition of a "record" maintained in a "system of records," the Act's notice access, correction, and accountability requirements do not apply to it.

In addition, there is no compatible-purpose test in the Act for internal agency uses of records; hence, such uses are unregulated. One exception is

---

account numbers pertaining to individual persons, [he] shall utilize exclusively the Social Security Act account numbers . . ." This was ordered "in the interest of economy and orderly administration." (See Chapter 16 for a more detailed discussion of this topic.)

the case in which there is a confidentiality statute governing the uses or disclosures of certain types of records of a particular component of an agency. Section 1106 of the Social Security Act was cited earlier as one such example. Unfortunately, however, the assortment of such confidentiality statutes is incomplete and uncoordinated.

Furthermore, it is probable, again because of technological advances, growth in government programs, and pressures to reduce paperwork, that the prediction of significant new uses of information will become even more difficult—and, hence, more difficult to deal with as a matter of public policy. A compromise which would achieve a reasonable balance between individual knowledge and agency efficiency concerns would seem to be in order.

The increased demand for information is changing the relationship between the record keeper and the record subject, as well as the character of the record-keeping relationship itself. As the Federal government has become increasingly involved in providing services and financial assistance, there have been increased pressures to ensure that all recipients are, in fact, eligible. This has led agencies into areas normally associated with civil or criminal law enforcement functions. In assessing this phenomenon, it must be remembered that much of what the agencies do in the area of record keeping and investigating is in response to direct or perceived mandates from the Legislative branch; in order to accomplish the tasks set for them, agencies need enforcement units with investigative capabilities. The recent creation of an office to investigate fraud and abuse in the Medicaid program provides an example of a unit which developed as a response to congressional direction.

Parallel to this increasing role for Federal agencies in law enforcement and investigative activities, the Federal government has begun to develop sophisticated criminal justice information systems, and to offer the services of those systems, as well as related technical and financial assistance, to State and local law enforcement agencies. While a number of questions need to be resolved in regard to this use of technologically sophisticated information systems by Federal or State law enforcement and investigative agencies, three problems are particularly pertinent to the protection of personal privacy.

The first emerges from even the briefest consideration of how information enters criminal justice information systems and how it is used. As such systems are currently structured, there is little control over the accuracy and reliability of information when it passes from one investigative agency to another. In particular, there is minimal control over the accuracy of criminal history information—often the most revealing and potentially the most damaging recorded information routinely exchanged by law enforcement agencies. The criminal history files of the FBI's Identification Division illustrate the inability of a central record keeper to control the quality of the information in its records, since by and large the central record keeper has little enforceable authority over other agencies reporting to it. [See *Menard v. Saxbe,* 498 F.2d 1017 (D.C. Cir. 1974)] Further, the information in such systems is ordinarily derivative; in other words, the

record maintained in an automated system is often copied from another record which in turn may be a copy of a third. The chances for error in transferring information from one record to another are great, particularly when the first transfer is from a paper record. These vulnerabilities to error create a system with inherent accuracy and reliability problems, but one which nonetheless is used to make decisions that affect individuals powerfully and immediately.

The second problem generated by these new systems grows out of the current pattern of unrestricted information flows between law enforcement and investigative agencies at all levels of government. Those flows, formal and informal, are usually justifiable, but they are also easily amenable to abuse. Easier access to information by agents within a unit, and greater facility to exchange information between units, will increase the potential for abuse and thus for the misapplications of police powers of the sort Americans experienced in the late 1960's and early 1970's. Moreover, the unsupervised information flows that facilitated improper domestic intelligence activities, and the government operations based on them, are still without oversight mechanisms to assure their accountability. As the deployment of technology increases the ease with which current information flows can be abused, the Congress should work rapidly to discover the extent and patterns of such flows and to develop statutorily mandated protections against their abuse.

The final problem that needs resolution results from Federal agencies providing computer-communications services to State and local law enforcement agencies. At one level, it is a classic problem of federalism, of the proper role of the central government in furnishing local services; at another level, however, it is a problem posed by one agency operating the information services on which other agencies depend and thus being able, at least potentially, to control the format of the other agencies' records and to use those records for its own purposes. Some of the consequences of a Federal law enforcement agency controlling the flow of State and local criminal justice information are illustrated in the continuing controversy over whether the Federal Bureau of Investigation should supply a message-switching, or interstate data communications, service through its National Crime Information Center (NCIC).

As the operator of NCIC, the FBI would exercise central control over, and have the ability to reach into, any State or local records that were directly hooked into the system, as well as the ability to monitor the flow of information through the system. While such an ability is only a potential, the transformation of that potential into an actuality has occurred before,[38] and would permit the agency controlling the system to collect and use information to which it might not be legitimately entitled. For example,

[38] Between April 1971 and February 1974 the FBI monitored requests for information in the NCIC made by State and local government agencies. The monitoring was conducted on behalf of the Department of Justice and other agencies of the Federal Government. The monitoring involved flagging the names of persons in whom the Federal agencies had some interest, including 4,700 who had no criminal record. In other words, any inquiry by a State or local government agency that included a flagged name was automatically noted and recorded for later examination by Federal agents. See letter of July 18, 1975, from Hon. John V. Tunney,

intelligence might be gathered on individuals whom the Administration in power considered politically undesirable, and be gathered by more sophisticated and comprehensive methods than those employed by the infamous Special Services Staff of the Internal Revenue Service.

Given the particularly damaging character of the information involved and the potential for misuse, any long-range decision to permit Federal agencies to provide such services should be made only if there is no alternative. Further, the Commission believes that the decision to permit Federal agency operation of such services ought to be made through the legislative process, not unilaterally by the Executive branch of government.

Perhaps the most significant finding in the Commission's assessment of the Privacy Act arises from its examination of the vehicles available for evaluating and assessing existing record systems, new systems, and agency practices and procedures. Quite simply, there is no vehicle for answering the question: "Should a particular record-keeping policy, practice, or system exist at all?" While the Act takes an important step in establishing a framework by which an individual may obtain and question the contents of his record, it does not purport to establish ethical standards or set limits to the collection or use of certain types of information. Without such standards, however, the principal threat of proliferating records systems is not addressed. Nowhere, other than in the ineffective section requiring the preparation and review of new system notices, does the Act address the question of who is to decide what and how information should be collected, and how it may be used. To deal with this situation, the Congress and the Executive Branch will have to take action.

U.S. Senator, to Hon. Harold Tyler, Deputy U.S. Attorney General; letter of August 29, 1975, from Hon. Harold Tyler to Hon. John V. Tunney.